FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1567457-000

Total Deleted Page(s) = 84
Page 32 ~ Duplicate;
Page 33 ~ Duplicate;
Page 34 ~ Duplicate;
Page 35 ~ Duplicate;
Page 36 ~ Duplicate;
Page 37 ~ Referral/Direct;
Page 38 ~ Referral/Direct;
Page 39 ~ Referral/Direct;
Page 40 ~ Referral/Direct;
Page 41 ~ Referral/Direct;
Page 42 ~ Referral/Direct;
Page 43 ~ Referral/Direct;
Page 51 ~ b3; b6; b7C; b7E;
Page 52 ~ b3; b6; b7C; b7E;
Page 84 ~ Duplicate;
Page 88 ~ Duplicate;
Page 89 ~ Duplicate;
Page 92 ~ Duplicate;
Page 93 ~ Duplicate;
Page 96 ~ b3; b6; b7C; b7D; b7E;
Page 97 ~ Duplicate;
Page 100 ~ b3; b6; b7C; b7D; b7E;
Page 101 ~ Duplicate;
Page 102 ~ Duplicate;
Page 104 ~ Duplicate;
Page 105 ~ Referral/Direct;
Page 106 ~ Referral/Direct;
Page 107 ~ Referral/Direct;
Page 109 ~ b6; b7C; b7E;
Page 110 ~ b6; b7C; b7E;
Page 113 ~ Duplicate;
Page 115 ~ b6; b7C; b7E;
Page 116 ~ b6; b7C; b7E;
Page 117 ~ b6; b7C; b7E;
Page 121 ~ Duplicate;
Page 126 ~ Duplicate;
Page 130 ~ Duplicate;
Page 131 ~ b3; b6; b7C; b7D; b7E;
Page 132 ~ b3; b6; b7C; b7D; b7E;
Page 133 ~ b3; b6; b7C; b7E;
Page 134 ~ b3; b7E;
Page 136 ~ b3; b6; b7C; b7E;
Page 140 ~ Duplicate;
Page 141 ~ Duplicate;
Page 145 ~ Referral/Direct;
Page 146 ~ Referral/Direct;
Page 147 ~ Referral/Direct;
Page 148 ~ Referral/Direct;
Page 149 ~ Referral/Direct;
Page 150 ~ Referral/Direct;
Page 151 ~ Referral/Direct;
Page 152 ~ Referral/Direct;
Page 153 ~ Referral/Direct;
Page 154 ~ Referral/Direct;
Page 155 ~ Referral/Direct;
Page 156 ~ b3; b6; b7C; b7E;
Page 158 ~ b3; b6; b7C;
Page 163 ~ Duplicate;
Page 164 ~ Duplicate;
Page 165 ~ Duplicate;
Page 166 ~ Duplicate;
Page 171 ~ Duplicate;
Page 172 ~ Duplicate;
Page 173 ~ Duplicate;
Page 174 ~ Duplicate;
Page 175 ~ Duplicate;
Page 194 ~ Duplicate;

Page 196 ~ Duplicate;
Page 197 ~ Duplicate;
Page 198 ~ Duplicate;
Page 199 ~ Duplicate;
Page 200 ~ Duplicate;
Page 201 ~ Duplicate;
Page 202 ~ d5;
Page 203 ~ d5;
Page 204 ~ d5;
Page 205 ~ d5;
Page 206 ~ d5;
Page 207 ~ d5;
Page 208 ~ d5;
Page 216 ~ Duplicate;
Page 220 ~ Duplicate;
Page 221 ~ Duplicate;
Page 222 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

CBS EVENING NEWS

Waging War With Computers

- *Experts Warn Threat Is Very Real*
- *U.S. Ill-Prepared To Battle Cyber-Terrorists*
- *CBS News Correspondent David Martin Reports*

Barnes and Noble.com THE STREET LAWYER by JOHN GRISHAM

CBS EVENING NEWS with DAN RATHER

"There is a transformation underway, away from the voyeurism that typified computer attacks in the past toward more serious and potentially dangerous things in the future."
Deputy Secretary of Defense John Hamre

CBS

OKLAHOMA CITY
Tuesday, May 26, 1998 - 08:24 PM ET

(CBS) They are 17 and call themselves Sniper and Solar—members of the hacker underworld.

VIDEO
CBS News Correspondent David Martin Reports On War Games

These kids use software with names like Satan and John the Ripper to break into government computers.

"It was just kinda to show the government that they're not as secure as they think," says the hacker who calls himself Sniper. **"This . . . right here is called Satan."**

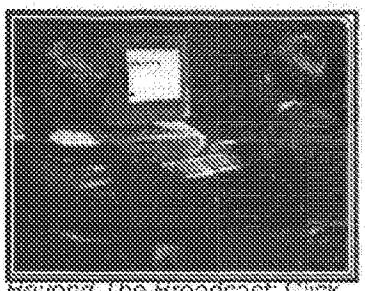
Click Here

Sniper and Solar don't go to school, but they understand in detail what most of us only dimly grasp. The United States—its transportation, its communications, its banking, its electrical power, its military—depends on computer networks that are vulnerable to what a presidential commission warned could be "a devastating attack."

If an enemy used a bomb to blow up the Defense computer center in Oklahoma City, it would be an act of war. But with cyber-war you don't need a bomb. You just use the Internet to infiltrate the system—erase files, redirect messages, turn order into chaos.

b6
b7C

b3
b6
b7C
b7E



Beyond The Broadcast: Click here for an interview with MOD hackers.(CBS)

The Pentagon found out how vulnerable it is to this type of attack last year, when a team of computer experts from the National Security Agency launched a mock cyber-attack. Had it been real, the assault would have knocked out power grids in cities with major military commands.

"It used to be easy not to worry about these kinds of attacks on the United States, because it would cost a lot for someone to send their army over to the United States to attack us," says Kathy Fifthen, who runs a computer emergency response team at Carnegie Mellon in Pittsburgh.

But the Internet has changed all that. Last year Fifthen's team handled more than 2,200 hacker attacks.

"On the Internet, there are no boundaries," Fifthen says. **"There's nothing to stop you from crossing the border."**

A teen-ager in Sweden used his laptop to flood the 911 service for much of Florida with bogus calls. The adolescent dream of getting into the school computer to change your grades has turned into a nightmare.

"Some students gained access to a hospital and actually changed medical records from cancer tests," Fifthen says. **"And women began undergoing cancer treatment, and then they found out that the records had been altered."**

Sniper and Solar say they haven't done anything like that, but they are part of a network of hackers who steal Pentagon software. They say their group has about 15 people. And it's an international effort, with members in Russia as well as the United States.

Bill Zane's Web page was hacked by a group of teenagers in California and Israel. "They trade the passwords that they've stolen, and they trade the software they use. And they're talking to each other, and they're bragging to each other," Zane says.

And worse, hackers are now talking about selling the software they steal from the government. **"There's a lot of people who'd like to get their hands on U.S. government software and ideas,"** Solar says.

"There might be like terrorists, people that want it and think that they can like shut down the United

States with it," adds Sniper.

Solar and Sniper swear they'd never do it, but John Vernessovich, who uses the Internet to talk to hackers all over the world, says the demand for their services is enormous.

"Dozens of people on a daily basis e-mail me wanting to know how they can get in touch with these people," he says.

Deputy Secretary of Defense John Hamre says that what started as a game of electronic gotcha has turned nasty and the stakes are getting higher.

"There is a transformation underway, away from the voyeurism that typified computer attacks in the past toward more serious and potentially dangerous things in the future," Hamre says.

"I believe within a year that we'll see hackers gain access to classified material," Vernessovich says.

As he scrolls through the electronic allies of the hacker underworld, Vernessovich can see with a few keystrokes what it took a presidential commission a year to figure out.

"The capability to do harm is real. It is growing at an alarming rate, and we have little defense against it," he says.

CBS News Correspondent David Martin. Copyright 1998, CBS Worldwide Inc., All Rights Reserved

RELATED STORIES
- Beyond The Broadcast

back to TOP

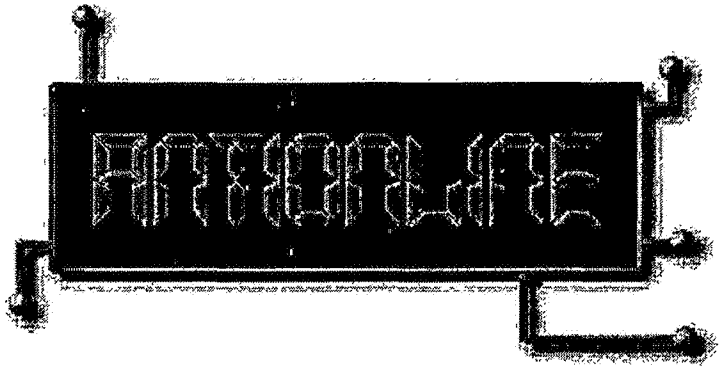
[Home | News | Weather | Sports | Life | Local Guide | Affiliates]
[Feedback | Help]

© 1998, CBS Worldwide Inc., All Rights Reserved.
Please click here for more copyright information.

CBS.com

ICON CUT CORP. ORACLE

Enter Company: go % change



"A Rick's Cafe in the Casablanca world of hacking." - ABC News

Email Address
Subscribe!

Back To AntiOnline

AntiOnline's Coverage Of The Defense Information Systems Network (DISN) Hackers Updated News Of The DISA Intrusions

The latest updated information shorts on the DISA attacks:

- DEM software authenticated by the DISA but found not to be classified.
- AntiOnline confirms 4 more DISA intrusions:
  - cheyenne.iiie.disa.mil
  - genesis.den.disa.mil
  - marble.inmspac.disa.mil
  - solbourne.c2del.disa.mil
- DISA Admin to hackers: "Come and get us I dare you to try!"
- MOD claims to have stolen submarine tracking software, and says it'll prove it in early may.

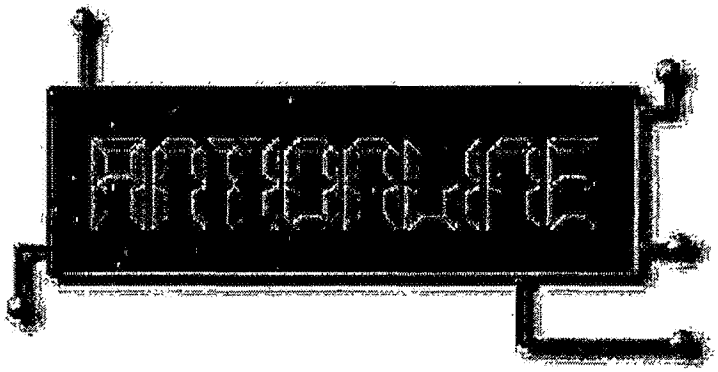
Full Stories Coming Soon...

Back To AntiOnline's Coverage Of The DISN Hackers

AntiOnline Is A Trademark Of John Vranesevich
Content Is © AntiOnline. All Rights Reserved

SCRAMBLED SERIALIZED
JUN 0 0 1998

Enter Company Microsoft go % change



"A Rick's Cafe in the Casablanca world of hacking." - ABC News

Email Address
Subscribe!

Back To AntiOnline

AntiOnline's Coverage Of
The Defense Information Systems Network (DISN)
Hackers
Comments From A Military Official

I am writing you with regards to the current exploits of the MOD hackers group, and my personal insights to the issue. I have been serving as a US Marine for almost six years, and my primary occupational specialty is to fix terrestrial satellite and microwave communications equipment. Namely the TRC-170, TSC-93A and TSC-85 suite and the CNCE (Communications Nodal Control Element). These systems provide satellite and microwave communications to deployed Marines and Sailors around the globe. In addition to my training I have officially lead or been involved with a number of computer initiatives within the Marine Corps and DoD. I am not familiar with the DEM program, but I am familiar with other systems like it. My current project is an initiative within the west coast portion of the Marine Corps (I MEF) to provide maintenance readiness data in a thin client/server relationship via TCP/IP and Banyan Vines, so that our deployed units can have a near realtime update of the current status of MEF readiness. This data contains a listing of every piece of equipment the MEF owns, and it's current status, such as things that are completly broken, kinda broken, or just missing a screw. With this system, if someone could gain access to it, they could give our warfighting status to terrorist organizations, yet this data is not classified. Of course common sense applies, it's probably not a good idea to advertise. While never laying eyes on the DEM program, I have a pretty good idea of what it contains, and what really happened. As I see it, some juvenille hackers found a hole in the DISA firewalls, and got on to some morons NT box, this idiot probably thought he knew everything, and was using his ftp to send files back and forth between work, even though his Sa had chewed his ass many times. These kids stumbled on to it, and made a big deal out of it. I"m not saying it's not a big deal, I mean we are supposed to have the most secure network in the world or something to that extent. In some cases we do, when we put up a secured system, we have hardware crypto computer to

computer, and any global traffic is encrypted between each point it travels, sometimes as much as three seperate translations. The cabling we use is a triple sheilded dual coax, with an unbelievibly low signal loss, it in itself is considered a secure mode of transmission. However, when it comes to the rear, and we let joe blow the average user have a 'white' pc, things get stupid fast. I personally know of several conditions that would allow someone easy access, with no hacking , to all of our systems. I think the media attention this group is getting is great, great for them in terms of exposure, and great for us in terms of education, funding, and policy. However, when the first response is to sell this data to terrorists or the like, I can't believe it, I can't condone it, it's just plain wrong. When these kids are caught, and they will be, they will hang, and no one will be there to support them.

f1shlips

Back To AntiOnline's Coverage Of The DISN Hackers

AntiOnline Is A Trademark Of John Vranesevich
Content Is © AntiOnline. All Rights Reserved

Enter Company go % change

"A Rick's Cafe in the Casablanca world of hacking." - ABC News

Email Address
Subscribe!

Back To AntiOnline

AntiOnline's Coverage Of The Defense Information Systems Network (DISN) Hackers NASA Computer Intrusion Detecton Software

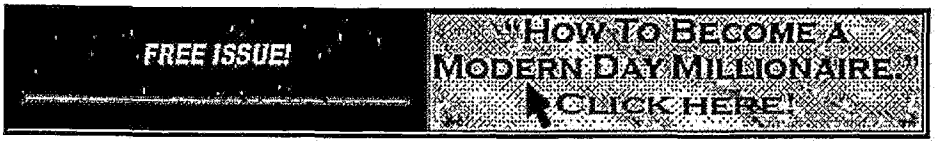
The hack group MOD claims in an exclusive interview with AntiOnline to have stolen software from "sensitive" NASA servers that are used to detect intrusions into their systems. "..with the intrusion detection programs, we know how to pass undetected through their systems" says a member of MOD who wishes to maintain his anonymity. The MOD has sent AntiOnline staff members "samples" of the unix based software packages that they have "acquired" from NASA. Below is a list of the different intrusion detection systems that the MOD has sent AntiOnline to date:

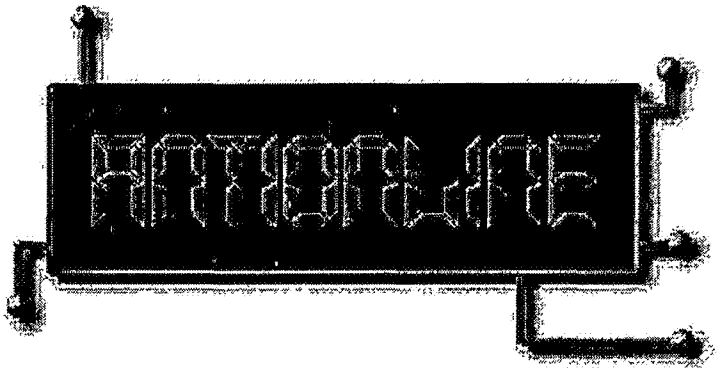
- NAIAD (Automated Inode Anomaly Detector)
- LARCSCAN
- SLIC (Scanner for Logfile InConsistencies)
- LASTLOG

Comments from MOD members and an examination of the programs and included files which were sent to AntiOnline, seem to point that these software packages are part of the NASIRC - NASA AUTOMATED SYSTEMS INCIDENT RESPONSE CAPABILITY. The NASIRC oversees data security for NASA installations such as NASA's Jet Propulsion Laboratory, the facility where the MOD claim to have stolen the software from. The MOD tell AntiOnline that this is just yet another small sample of data and access that they have gathered from US Military and Governmental servers in the past year.

Back To AntiOnline's Coverage Of The DISN Hackers

AntiOnline Is A Trademark Of John Vranesevich





"A Rick's Cafe in the Casablanca world of hacking." - ABC News

Email Address
Subscribe!

Back To AntiOnline

AntiOnline's Coverage Of The Defense Information Systems Network (DISN) Hackers Who Are The MOD? What Are Their Goals?

The MOD (Masters Of Downloading/2016216) as they jokingly call themselves, are a group of approximately 15 hackers. They hackers come from the United States (8), UK (5), and Russia (2). Below is an interview John Vranesevich (JP) had with one of the members of MOD(note this is a log from an IRC Session. The hacker that was interviewed asked that no information be disclosed about him, not even his handle. For the purposes of this log, we will refer to this hacker by the name of his group, MOD.):

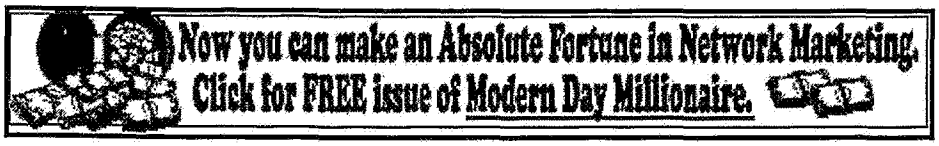
JP - Why did you guys break into the systems in the first place?
MOD - it was a challenge
MOD - and we wanted to try and find some classified data
MOD - not your usual webpage stuff
JP - so why did you want to go after classified materials?
MOD - because classified materials are generally more of a challenge
MOD - and reap larger rewards
JP - what made you decide to go after the DISN and not the pentagon itself?
JP - or nasa for that matter?
MOD - we have already done NASA
MOD - but that was a long time ago
MOD - and people got busted
JP - did you gain any classified materials from it?
MOD - we gained no classified materials, but the FBI seemed to think we did
MOD - we broke into the jet propulsion labs
MOD - they have satellite inf0 there
MOD - anyway...
MOD - the pentagon is part of the DISN
MOD - and the DISA are the responsible party for the well-being of the

DISN
MOD - that's why we went for the DISA
MOD - all very logical
MOD - all the _real_ pentagon systems use the old networks anyway
MOD - x.25
MOD - etc.
JP - why did you wait 6 months to come forward with the stolen software?
MOD - we wanted to make absolutely sure that the DISA hadn't busted anyone
MOD - I personally wanted to release the software when we got it
MOD - the DISA shut down a few of the ftp sites it was stored on days after
MOD - I am perfectly sure the cost is clear
MOD - I have been for months
MOD - It's the guys in the US who are more likely to get busted over this
MOD - and that's why we have waited
JP - are there other things that your group is holding until your sure the "coast is clear" ?
MOD - We have other classified data and access to networks
MOD - so we are still at large
MOD - I personally am getting a bit too busy with work/real life issues to be playing God with the US DoD's networks
MOD - But the Russians I know for a fact still have alot of access to classified data
MOD - That's a whole different story.. :-)
JP - When you say "The Russians", you're referring to the russian members of your group?
MOD - yes
JP - people like The Analyzer have been criticized for using commonly known exploits to gain access to US military and governmental servers. Did your group use similar exploits?
MOD - It was a case of finding weak links in networked environments, using many techniques..
MOD - We have non-public local and remote exploits
JP - Do any members of your group work with/for foreign governmental or military agencies?
MOD - No
MOD - None of us work for any agencies or governments
MOD - heh
MOD - I am pretty sure we are all employed to do security related work
JP - Will your group continue to infiltrate high-level US governmental and military servers?
MOD - yes, and non-governmental servers
JP - Could you name some examples of commercial or educational servers your group as infiltrated?
MOD - we have infiltrated many systems based in eastern europe and asia
MOD - we have scanned all of hungary, switzerland, japan and thailand for remote holes such as imap,statd,cgi's,nfs exports
JP - Ok, let's talk a bit about the software package that you recovered from the DISA.
JP - what was it called?
MOD - it is called DEM
JP - and that stands for what?

MOD - the DISN Equipment Manager
MOD - DISN stands for Defense Information Systems Network
JP - What does your group believe this software is/was used for?
MOD - It was used by the DISA to routinely check and maintain the DISN hardware from a remote location
MOD - that hardware being routers, multiplexers, IDNX networks, repeaters
MOD - and GPS satellites and receivers
JP - Does your group believe it would be able to use this software to disable military data networks
MOD - Since we have had the software we have taken it apart to analyze it's function further
MOD - We believe that with a spoofed machine, or from a disa.mil IP (if we hacked the nameservers), that we could remotely reconfigure such hardware
JP - Does your group have any intentions of doing so?
MOD - It is always nice to have such power over a network as big and valuable as the DISN
MOD - but at this point in time, we'd just like this to be a reminder to the US DoD that we can take down their entire network from a remote location
MOD - ie. anywhere on the earth's surface
MOD - we have the power to do so, but at this point in time, we have no reason to launch such an attack..
JP - Dont' you think they would have made changes to their network after knowning that this software has been stolen?
MOD - after we stole the software, they spent ALOT of money in securing the NT cluster that we had infiltrated
MOD - if we _really_ wanted to, I'm sure we could get back into those machines.. but it would take some time, it would be a full-time operation.
MOD - we have non-public local and remote exploits
MOD - all we have to do is compromise an account
MOD - and we are back in..
MOD - however I think we have already proven our point
MOD - purely by stealing classified material from the DoD over the internet
MOD - we have alot more pressing projects to undertake now, regarding china and other countries..
MOD - as they also have defense networks
MOD - we are not stupid enough to re-prove our point and risk getting caught
MOD - we would rather target new defense networks
MOD - but I don't want to go into that right now..
JP - What do you think governments and military institutions should be doing to ensure the security of their networks?
MOD - it's simple
MOD - 1) take all military systems off the internet
MOD - 2) place only military webservers on the internet
MOD - keep the rest on a purely internal network
JP - Well, government officials have already told the public that the most classified of data is kept on a purely internal network.
JP - Do you believe this?
MOD - I believe we have clearly proven that is not true..

Back To AntiOnline's Coverage Of The DISN Hackers

AntiOnline Is A Trademark Of John Vranesevich
Content Is © AntiOnline. All Rights Reserved



"A Rick's Cafe in the Casablanca world of hacking." - ABC News

Email Address
Subscribe!

Back To AntiOnline

AntiOnline's Coverage Of
The Defense Information Systems Network (DISN)
Hackers
John Vranesevich's Second Interview With MOD Members

Once again, the hackers asked that no information be released about them. We will refer to these two hackers by their group name as well, MOD and MOD2.

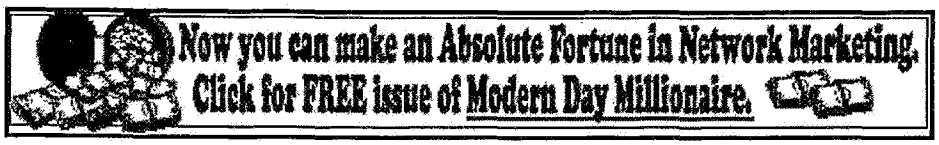
JP - how long has your group been around?
MOD2 - we have been hacking for over a year
MOD2 - as a group
MOD - yeah
JP - what is your goal as a group?
JP - your mission so to speak?
MOD2 - our mission is to set challenges in breaking networked systems globally
MOD2 - sometimes we succeed in our missions, and end up with classified information :)
JP - have you ever defaced a US webpage?
MOD - we haven't defaced any pages as MOD
MOD2 - no
MOD2 - we have better things to do :)
MOD2 - we could break pages all day, but we wouldn't get many classified programs
JP - is DEM the only piece of .mil software you've gained access to?
MOD2 - DEM isn't the only piece of american military software we have access to, we have also stolen security programs from NASA and stuff
MOD - DEM is very dangerous in the wrong hands.. :-)
JP - what type of nasa security programs?
MOD2 - security programs used for intrusion detection etc.
MOD2 - but with the intrusion detection programs, we know how to pass undetected through their systems

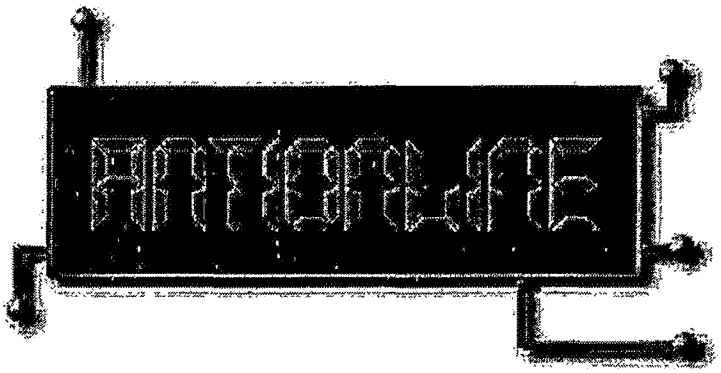
JP - are they *.nix or win based?
MOD2 - they are unix based
MOD2 - we stole DEM 6 months ago now..
MOD - yeah
MOD - we have been doing alot of work with systems in europe and asia
JP - Here's a stock media question for you. If you could send one message to the US government, what would it be?
MOD2 - "You cannot defeat the machine."
MOD - hahahaha
MOD - that's the best quote i've heard in a long time
JP - do any of you think you'll ever be caught?
MOD2 - JP : we have non-public remote and local exploits, we are unlike any of your normal hacker kids..
MOD - we will never get caught, because we don't make mistakes.
MOD2 - JP : myself and MOD are employed as computer security consultants.. i think it's fair to say we have the skills necessary to break into such systems.
JP - what are some future planned targets?
JP - generally speaking of course
MOD2 - we have already started some major work in europe and asia
MOD2 - we are looking into information warfare exercises against more network-dependant countries, like singapore and japan..
MOD - yeah
MOD - we want to shut down tokyo
MOD2 - seriously though, we are looking into such exercises..
MOD - but for now, we are just continuing to exploit and backdoor networks in europe and asia
MOD - we must have around 400 systems fully backdoored worldwide
MOD2 - i think it's more than 400 MOD. i'll count them later
MOD - well
MOD - it's a fucking lot
JP - well, how are you sure that the DEM software is classified?
MOD - because the DISA run the DISN, we thought it would be a more fruitful target than the pentagon networks..
MOD2 - we are not sure the software is classified, but we are sure we stole it from disa.mil, from where they control the entire DISN
MOD2 - any tool that allows us to retrieve data from military satellites must be worth quite alot though
MOD2 - it gives the exact position of the satellite
MOD2 - you can also toggle between satellites
MOD2 - it's very dangerous in the wrong hands
MOD2 - we could take apart the DEM software to find the systems it connects to, and then ping flood those systems from oc3 shells, thus disabling the ground based GPS receivers
JP - were you able to recover any other files or programs from disa.mil or just the DEM?
MOD2 - we stole alot from the defense information systems agency
JP - such as?
MOD2 - we retreived reports, logs of people using the machines
MOD2 - nothing special
JP - what type of reports?
MOD2 - reports on the status of routers and equipment
MOD2 - and networking
MOD2 - we had network topologies for systems in the pacific and hawaii
MOD - we have full root access to systems on backbones in us,

hungary, greece, thailand, japan and china, around 350 in total.
MOD2 - we still have alot of access to military networks
JP - what do you plan to do with all this data your gaining access to?
MOD2 - release it
MOD2 - or sell it..
JP - to whom?
JP - governments?
MOD - i think international terrorist groups would be interested in the data we could gain access to
MOD2 - governments would buy it for intelligence purposes
MOD2 - we're not your normal hacker kids

Back To AntiOnline's Coverage Of The DISN Hackers

AntiOnline Is A Trademark Of John Vranesevich
Content Is © AntiOnline. All Rights Reserved





"A Rick's Cafe in the Casablanca world of hacking." - ABC News

Email Address
Subscribe!

Back To AntiOnline

AntiOnline's Coverage Of The Defense Information Systems Network (DISN) Hackers
AntiOnline's Exclusive ScreenShots Of The DEM Software

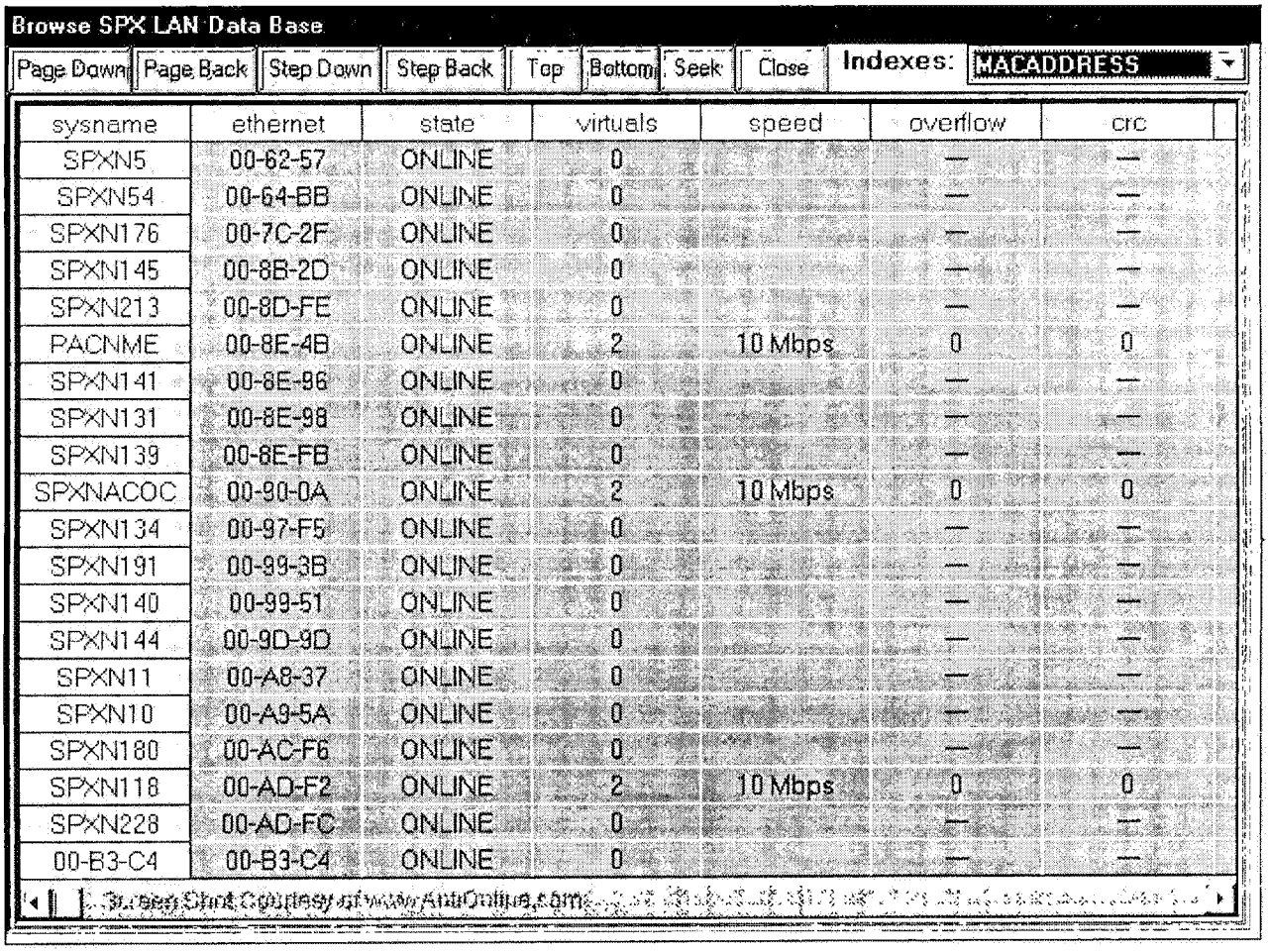
In an astonishing move, the MOD sent AntiOnline the actual program that they recovered from a DISN server. We have now made the decision, after talking with the MOD, to release to the public screen shots of this actual sotware being run. Please Note: When this program was run, it was run "offline" so that it did not attempt to make contact with any military servers, or hardware devices. Because of this, you will see that many of the data fields are blank. Also Note: There are aspects and menus of this program that we have chosen not to publish screenshots of.

- The DISN Equipment Manager - Main Menu
- The DISN Equipment Manager - Program Settings
- The DISN Equipment Manager - Database Stats
- The DISN Equipment Manager - Echo Canceller
- The DISN Equipment Manager - GPS Receiver
- The DISN Equipment Manager - UPS Stats
- The DISN Equipment Manager - SPX Lan Database

Other Software Stats:

- The Software package is around 18megs when fully installed.
- There are nearly 245 seperate files in 17 different folders that make up the software suite.
- The software requires a user to enter a login and password before it can be used.

Back To AntiOnline's Coverage Of The DISN Hackers

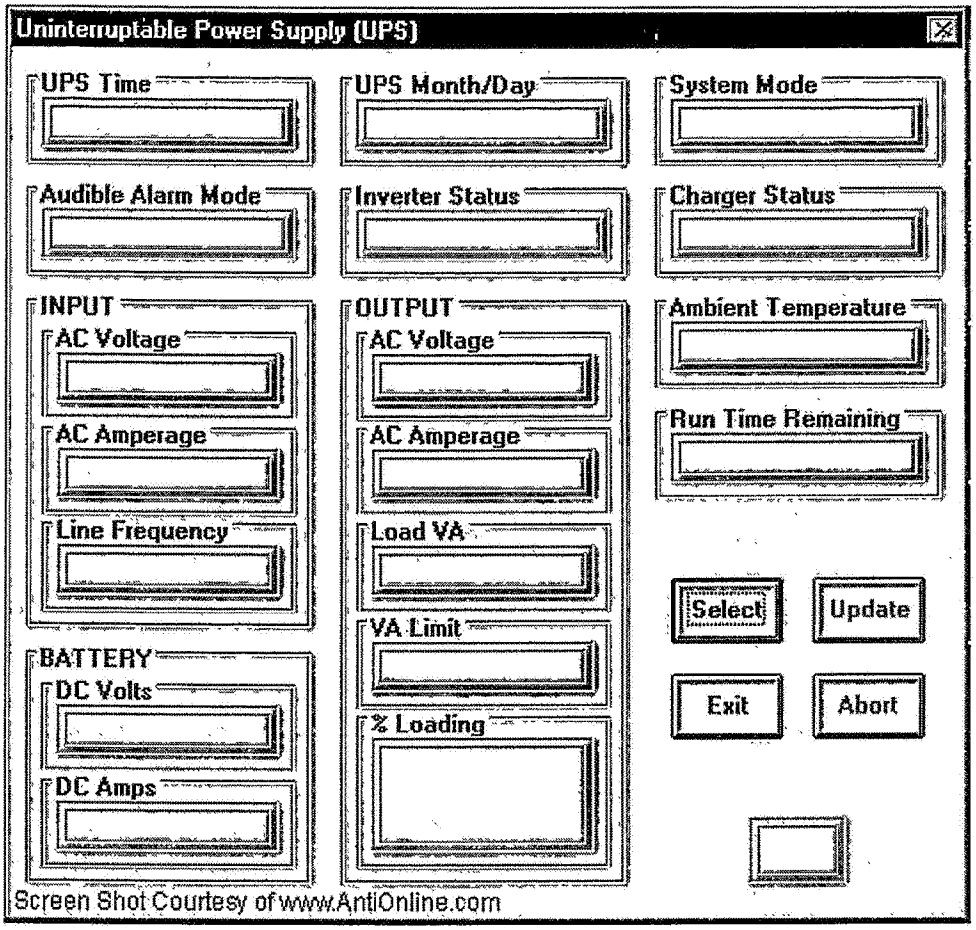


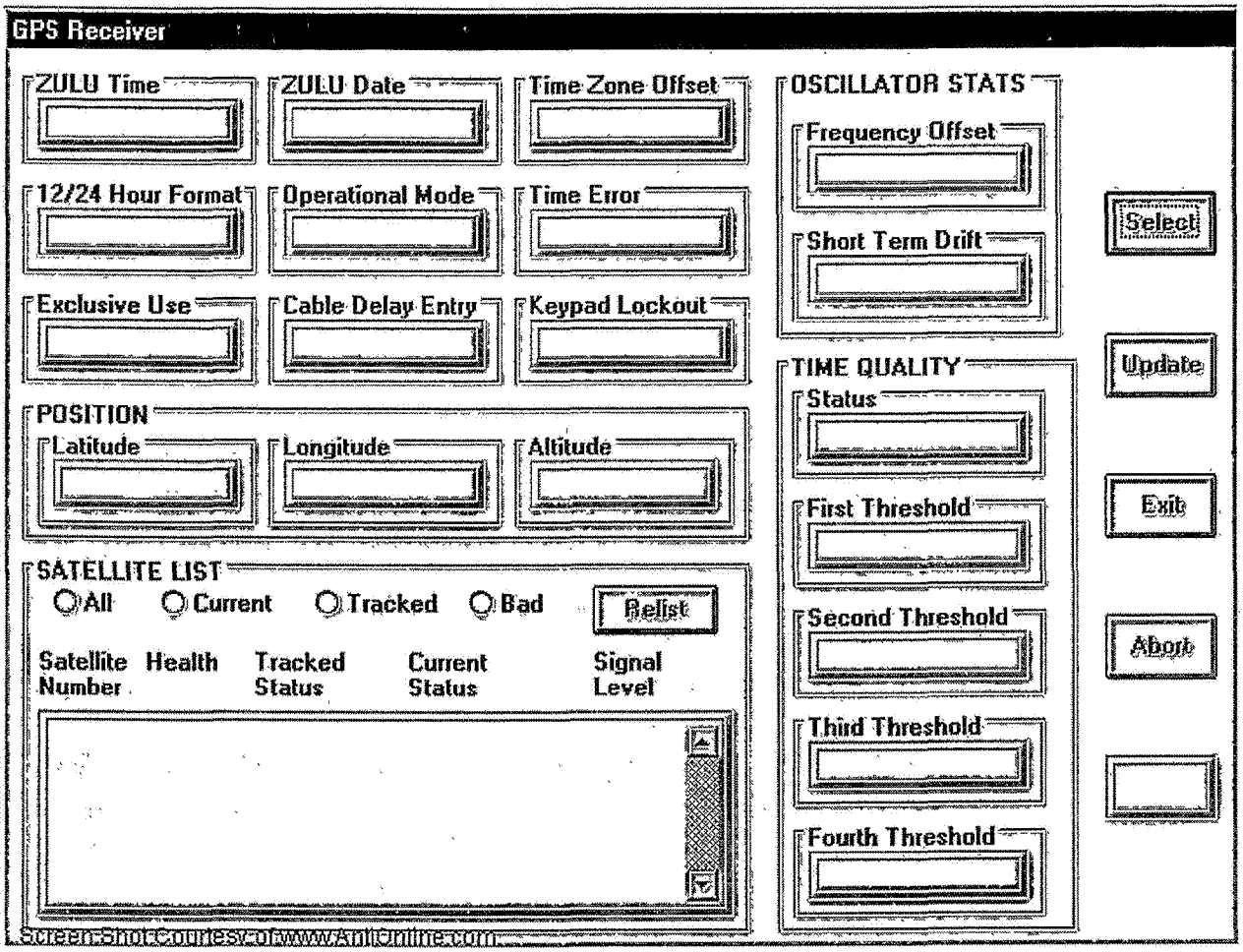
Browse SPX LAN Data Base

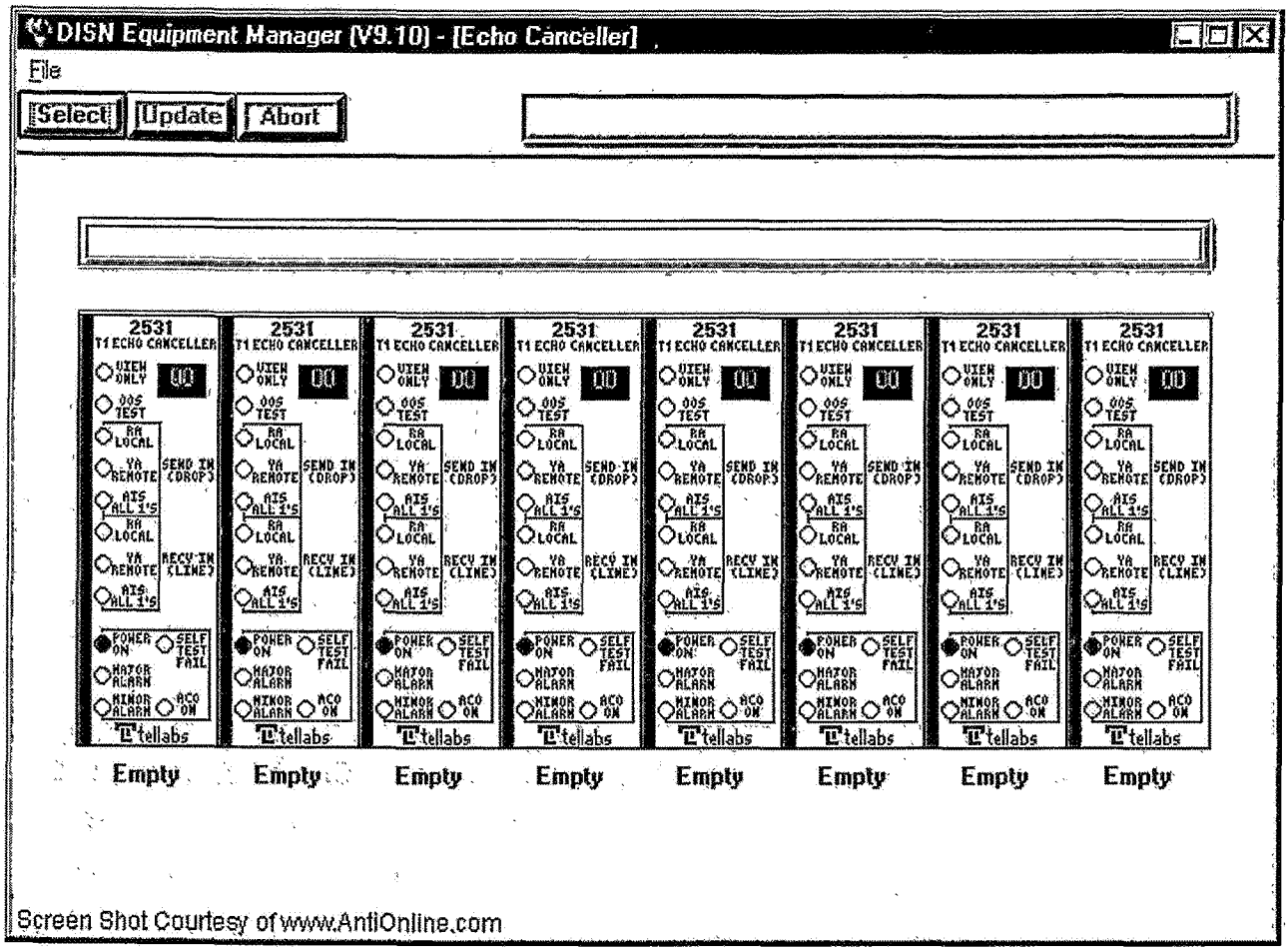
Page Down | Page Back | Step Down | Step Back | Top | Bottom | Seek | Close | Indexes: MACADDRESS

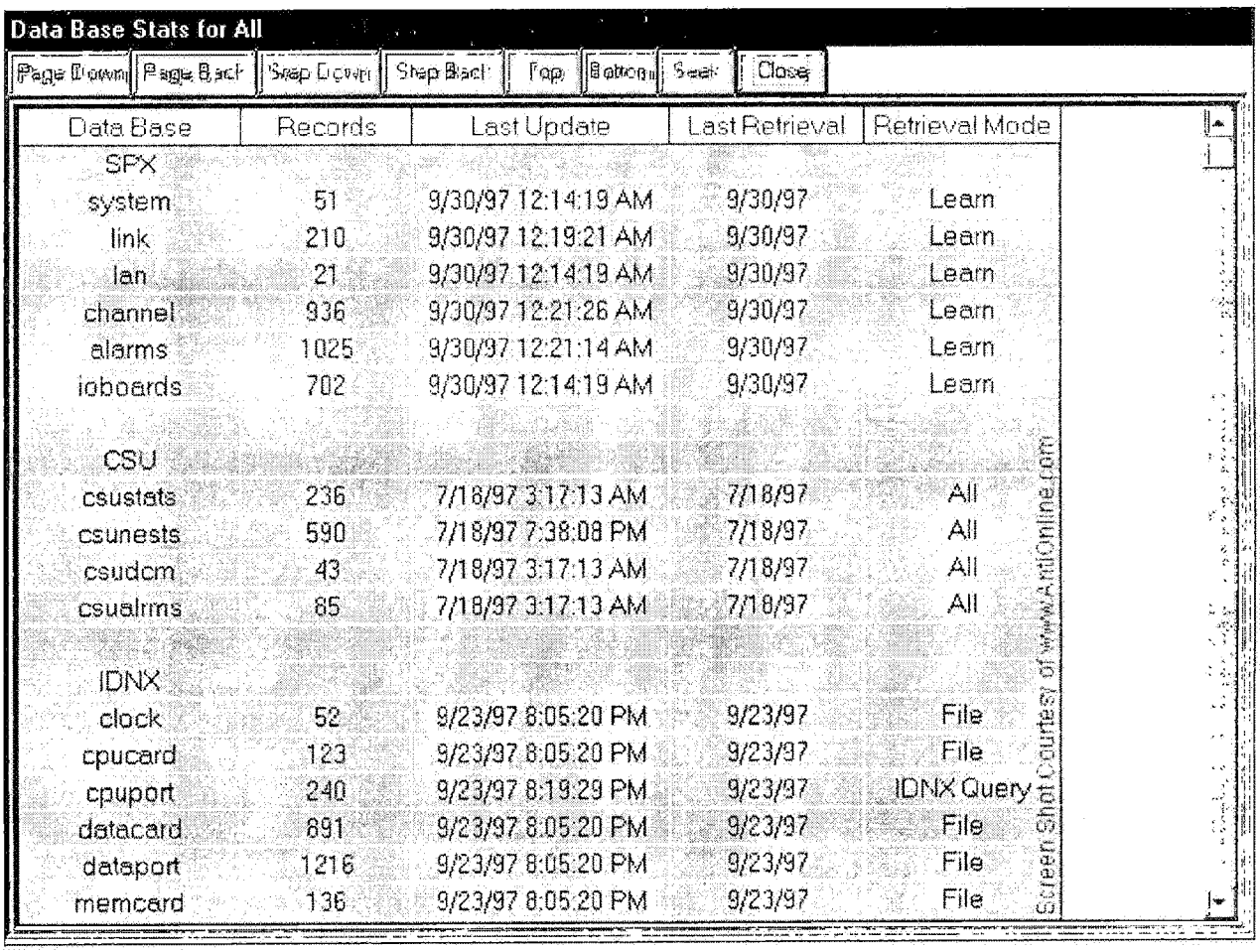
sysname	ethernet	state	virtuals	speed	overflow	crc
SPXN5	00-62-57	ONLINE	0		—	—
SPXN54	00-64-BB	ONLINE	0		—	—
SPXN176	00-7C-2F	ONLINE	0		—	—
SPXN145	00-8B-2D	ONLINE	0		—	—
SPXN213	00-8D-FE	ONLINE	0		—	—
PACNME	00-8E-4B	ONLINE	2	10 Mbps	0	0
SPXN141	00-8E-96	ONLINE	0		—	—
SPXN131	00-8E-98	ONLINE	0		—	—
SPXN139	00-8E-FB	ONLINE	0		—	—
SPXNACOC	00-90-0A	ONLINE	2	10 Mbps	0	0
SPXN134	00-97-F5	ONLINE	0		—	—
SPXN191	00-99-3B	ONLINE	0		—	—
SPXN140	00-99-51	ONLINE	0		—	—
SPXN144	00-9D-9D	ONLINE	0		—	—
SPXN11	00-A8-37	ONLINE	0		—	—
SPXN10	00-A9-5A	ONLINE	0		—	—
SPXN180	00-AC-F6	ONLINE	0		—	—
SPXN118	00-AD-F2	ONLINE	2	10 Mbps	0	0
SPXN228	00-AD-FC	ONLINE	0		—	—
00-B3-C4	00-B3-C4	ONLINE	0		—	—

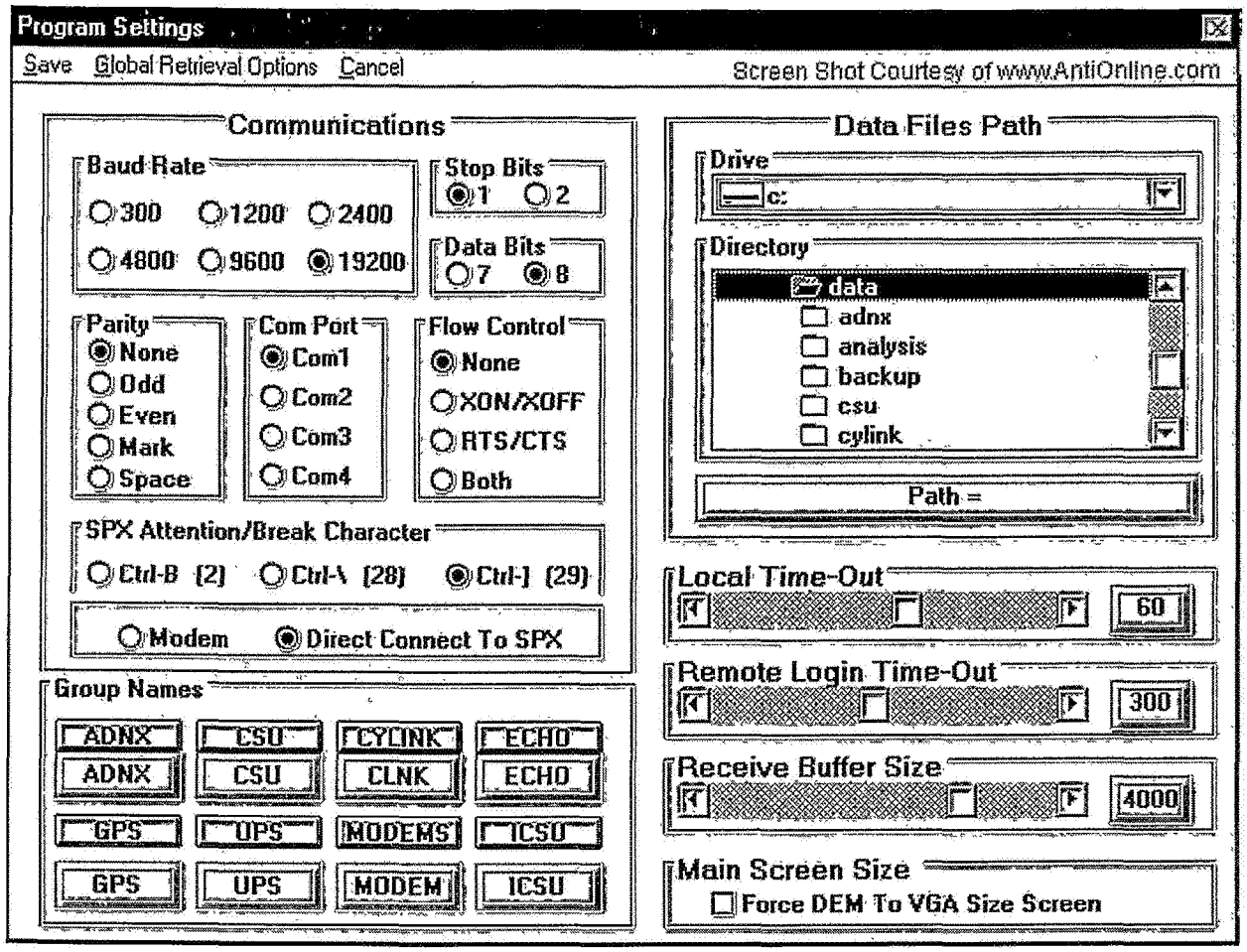
Screen Shot Courtesy of www.AntiOnline.com

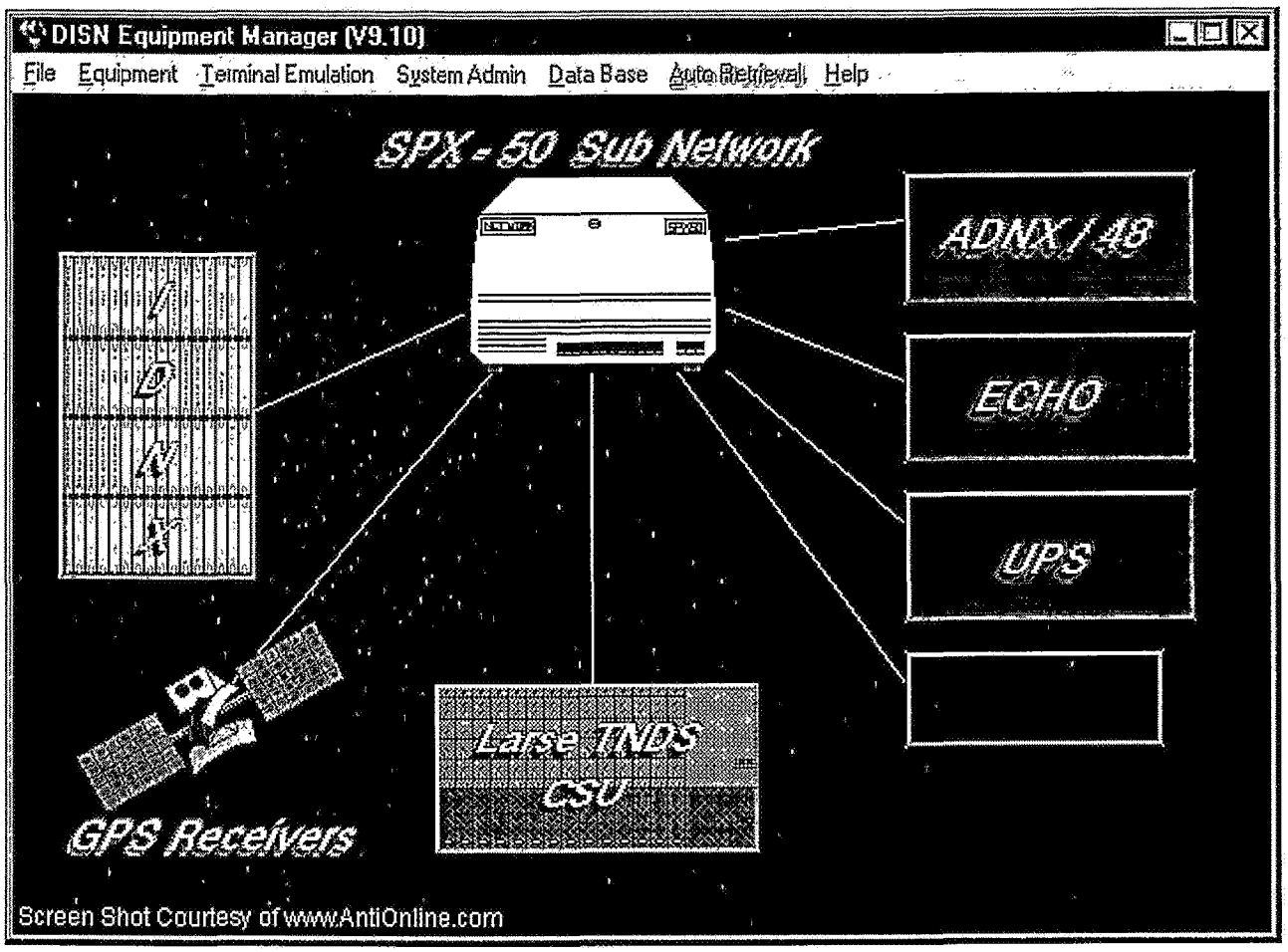

Uninterruptable Power Supply (UPS)
UPS Time
UPS Month/Day
System Mode
Audible Alarm Mode
Inverter Status
Charger Status
INPUT
AC Voltage
AC Amperage
Line Frequency
BATTERY
DC Volts
DC Amps
OUTPUT
AC Voltage
AC Amperage
Load VA
VA Limit
% Loading
Ambient Temperature
Run Time Remaining
Select
Update
Exit
Abort
Screen Shot Courtesy of www.AntiOnline.com

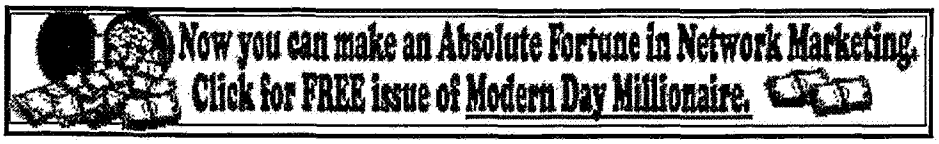

GPS Receiver
ZULU Time
ZULU Date
Time Zone Offset
12/24 Hour Format
Operational Mode
Time Error
Exclusive Use
Cable Delay Entry
Keypad Lockout
POSITION
Latitude
Longitude
Altitude
SATELLITE LIST
All
Current
Tracked
Bad
Relist
Satellite Number
Health
Tracked Status
Current Status
Signal Level
OSCILLATOR STATS
Frequency Offset
Short Term Drift
TIME QUALITY
Status
First Threshold
Second Threshold
Third Threshold
Fourth Threshold
Select
Update
Exit
Abort
Screen Shot Courtesy of www.AntiOnline.com

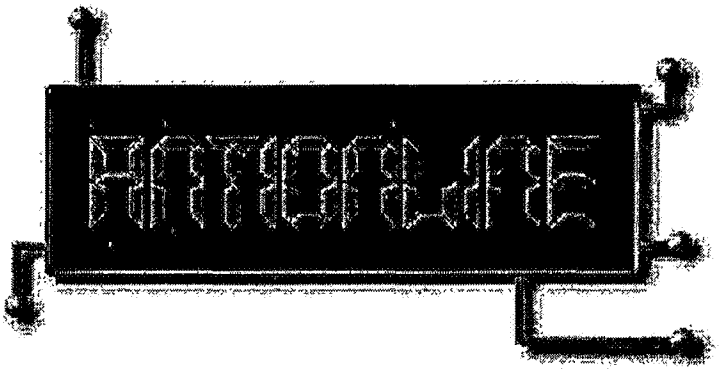

DISN Equipment Manager (V9.10) - [Echo Canceller]
File
Select
Update
Abort
2531
T1 ECHO CANCELLER
Empty
Screen Shot Courtesy of www.AntiOnline.com


Data Base Stats for All
Page Down
Page Back
Step Down
Step Back
Top
Bottom
Seek
Close
Data Base
Records
Last Update
Last Retrieval
Retrieval Mode
SPX
system 51 9/30/97 12:14:19 AM 9/30/97 Learn
link 210 9/30/97 12:19:21 AM 9/30/97 Learn
lan 21 9/30/97 12:14:19 AM 9/30/97 Learn
channel 936 9/30/97 12:21:26 AM 9/30/97 Learn
alarms 1025 9/30/97 12:21:14 AM 9/30/97 Learn
ioboards 702 9/30/97 12:14:19 AM 9/30/97 Learn
CSU
csustats 236 7/18/97 3:17:13 AM 7/18/97 All
csunests 590 7/18/97 7:38:08 PM 7/18/97 All
csudcm 43 7/18/97 3:17:13 AM 7/18/97 All
csualrms 85 7/18/97 3:17:13 AM 7/18/97 All
IDNX
clock 52 9/23/97 8:05:20 PM 9/23/97 File
cpucard 123 9/23/97 8:05:20 PM 9/23/97 File
cpuport 240 9/23/97 8:19:29 PM 9/23/97 IDNX Query
datacard 891 9/23/97 8:05:20 PM 9/23/97 File
dataport 1216 9/23/97 8:05:20 PM 9/23/97 File
memcard 136 9/23/97 8:05:20 PM 9/23/97 File
Screen Shot Courtesy of www.AntiOnline.com


Program Settings
Save
Global Retrieval Options
Cancel
Screen Shot Courtesy of www.AntiOnline.com
Communications
Baud Rate
300
1200
2400
4800
9600
19200
Stop Bits
1
2
Data Bits
7
8
Parity
None
Odd
Even
Mark
Space
Com Port
Com1
Com2
Com3
Com4
Flow Control
None
XON/XOFF
RTS/CTS
Both
SPX Attention/Break Character
Ctrl-B [2]
Ctrl-\ [28]
Ctrl-] [29]
Modem
Direct Connect To SPX
Group Names
ADNX
CSU
CYLINK
ECHO
ADNX
CSU
CLNK
ECHO
GPS
UPS
MODEMS
ICSU
GPS
UPS
MODEM
ICSU
Data Files Path
Drive
c:
Directory
data
adnx
analysis
backup
csu
cylink
Path =
Local Time-Out
60
Remote Login Time-Out
300
Receive Buffer Size
4000
Main Screen Size
Force DEM To VGA Size Screen


DISN Equipment Manager (V9.10)
File Equipment Terminal Emulation System Admin Data Base Auto Retrieval Help
SPX - 50 Sub Network
ADNX / 48
ECHO
UPS
Larse TNDS CSU
GPS Receivers
Screen Shot Courtesy of www.AntiOnline.com





"A Rick's Cafe in the Casablanca world of hacking." - ABC News

Email Address
Subscribe!

Back To AntiOnline

AntiOnline's Coverage Of The Defense Information Systems Network (DISN) Hackers How Did AntiOnline Verify This Story?

We at AntiOnline always feel that it's necessary for us to publish a "How Did We Verify" note with every major story we break. We think it's important for two reasons. First, we realize that we are not a major, mainstream media outlet. We don't have the type of reputation as some of the nation's largest newpapers and television networks do (although if we keep breaking major stories like this, we're liable to get one in a hurry ;). Secondly, because the Internet is still such a new and foreign concept to most, we feel that it's important to explain to people how information can be validated just as conclusively in cyberspace, as it can be in the real world.

Step One:
How do we know that a hacker is really who he claims to be? Well, this is sometimes the most challenging part. AntiOnline has an extensive database of information about hackers and groups. Things like, their handles, the hostmask (user@domain) that they often appear from, and their phone number if they choose to give it to us. In some cases, hackers, system admins, and yes, even reporters will setup password phrases with us, so that we can verify one another in the future.

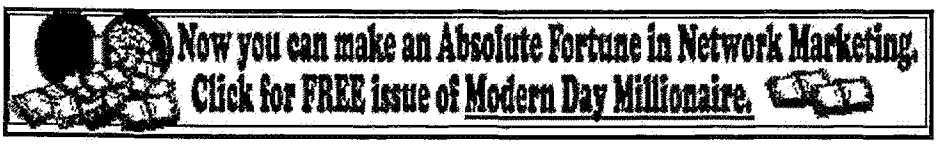
Step Two:
How do we verify that a hack has occured, and that the hacker that's taking credit for it, is the same one who hacked it? This is two fold. First off, this is where the mainstream media helps us out alot. Places such as Wired News (big thumbs up to the wired crew!) have contacts with big companies and governmental agencies (just as we have contacts with "underground" people), and are often very helpful in this respect. We can take the info. from them, put it together with info we get, and can usually get a pretty clear, reliable picture of what really occured. If we're not 100% sure about something, we don't publish it,

that simple.

Step Three:
This comes with just "being around". We have been on the scene for a long time. We've gotten to know people. We know who can be trusted, who can not. We know what's technically possible, and what is not. Put this together with steps one and two, and you get the winning combination =)

Back To AntiOnline's Coverage Of The DISN Hackers

AntiOnline Is A Trademark Of John Vranesevich
Content Is © AntiOnline. All Rights Reserved



"A Rick's Cafe in the Casablanca world of hacking." - ABC News

Email Address
Subscribe!

AntiOnline's Coverage Of The Defense Information Systems Network (DISN) Hackers

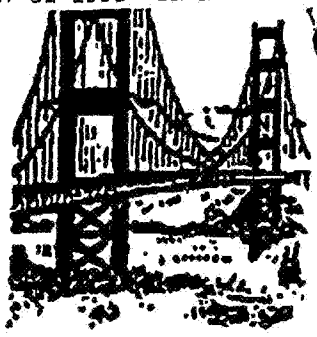
Back To AntiOnline

Loze Link
Little Games

In October of 1997, an elite group of around 15 hackers set out to gain access to The Defense Information Systems Network. In what may now be the first publicly known case of a high level US Military Computer Intrusion, the MOD talk exclusively to AntiOnline about their assult against the DISN, and what they found when they gained access. We will be posting more details here as we get them.

- **AntiOnline Threatened By The DISA** (5/04/98)
- **Updated Info. and Facts Of The DISA Hacks** (4/23/98)
- **Comments To AntiOnline From A Military Official** (4/22/98)
- **MOD Reveals Details Of NASA Computer Intrusion Detection Software** (4/22/98)
- **Who Are The MOD? What Are Their Goals? - JP's Interview With A MOD Member**
- **Second Interview With Other Members Of The MOD**
- **AntiOnline's Exclusive ScreenShots Of The DEM Software**
- **Links to Other Sites That Are Related To This Story** (updated 4/22/98)
- **How Does AntiOnline Verify Its Stories?**

AntiOnline Is A Trademark Of John Vranesevich
Content Is © AntiOnline. All Rights Reserved



FBI FACSIMILE

COVER SHEET

PRECEDENCE

- ☐ Immediate
- ☑ Priority
- ☐ Routine

CLASSIFICATION

- ☐ Top Secret
- ☐ Secret
- ☐ Confidential
- ☐ Sensitive
- ☑ Unclassified

Time Transmitted: 1639
Sender's Initials:
Number of Pages: 11
(including cover sheet)

☒

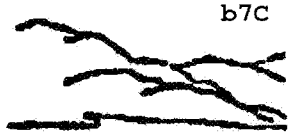
To: FBI HQ NIPC
Name of Office

Date: 30 APR 98

Facsimile Number: (202) 324-0311

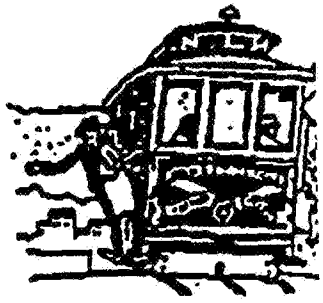
Attn: SSA
Name Room Telephone

b6
b7C



From: San Francisco
Name of Office

Subject: The Queen by SA



Special Handling Instructions:

Originator's Name: SA Telephone: x2518

b3
b6
b7C

Originator's Facsimile Number: (415) 553-7674

b7E

Approved:

Brief Description of Communication Faxed: Reading of online Queen

JUN 0 [illegible] 1998

WARNING

Information attached to the cover sheet is U.S. Government Property. If you are not the intended recipient of this information, disclosure, reproduction, distribution, or use of this information is prohibited (18.USC. § 641). Please notify the originator or local FBI Office immediately to arrange for proper disposition.

Untitled

4/30/98
1605 PDT
IRC Server: ircnet.sprynet.com
IRC Network: Internet Relay Network

Reliable →
Nickname: [redacted]
Email: [redacted]
Real name/URL: [redacted]
Channel(s): [redacted]
Server: [redacted]
Idle time: Unknown
Away: No
IRC Operator: No

b6
b7C

DIG hostname->ipaddress results.

Click on your browser's <Back> button to return to previous page.

b6
b7C

FINGER user@hostname results.

Click on your browser's <Back> button to return to previous page.

Finger na [redacted]

b6
b7C

Fingers are not permitted from outside

FINGER user@hostname results.

Click on your browser's <Back> button to return to previous page.

[redacted] b6 b7C

Finger na[redacted]

Traceroute

TRACEROUTE hostname results.

Click on your browser's <Back> button to return to previous page.

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	

b6
b7C

Crackers Set Sights on Submarines

by James Glave

5:02am 24.Apr.98.PDT

The cracker group that claimed earlier this week to have stolen US Department of Defense networking software is gearing up to release another suite of sensitive programs.

The group, called Masters of Downloading, or MOD, say that on 1 or 2 May they will release a set of programs used to track and communicate with submarines.

In an Internet relay chat interview Thursday with Wired News, a 24-year-old Russian member of MOD said the group will release the submarine programs, "and more after that." He declined to identify himself and he would not elaborate on what the sub programs actually do -- stating only that "we have so much more to show you."

"Information warfare is a very genuine threat," said the cracker, who claimed his group pilfered the networking software from a Windows NT server at the Defense Information Systems Agency (DISA).

Yesterday, a DISA spokeswoman said that the theft of the software, called the Defense Information Systems Network Equipment Manager (DEM), in no way represented a threat to national security.

"There is no national security risk posed by this being in the wrong hands," said Betsey Flood, who added that the intrusion was being treated as a "serious matter."

"The software is an unclassified application, it does not contain classified information, and it does not perform control of classified systems," said Flood.

But the MOD member said that DISA was playing down the threat.

"The DEM may be unclassified, but the information it can give can lead to highly classified data being compromised," the cracker said.

"The fact that [the DEM software] was fully configured makes all the difference -- we know the servers and networks that it connects to and we also had a lot of logs and generated reports from when it was run previously," he said.

To prove his point, he outlined exactly how the configured software could be exploited.

"We could launch the DEM program using the DISA systems as a trusted gateway, thus gaining very important router/repeater information about the DISA," he said.

TECHNOLOGY
Today's Headlines

All-in-One DSL Modem Chips

Net Access via Apartment LANs

AntiOnline Founder Under Fire

Should Feds Trust Windows NT?

The Case of the Mistaken Spammer

OpenCable Progress Told

The Electronic Nose Knows

Networking Consumer Gadgets

Mining the Moon for Habitation

Small and Slow ... but Clean

Pumping Plastic

The Sound of Poison

b6
b7C

b3
b6
b7C
b7E

JUN 0 1998

AM

"We could then either reconfigure/shut down the equipment, or attempt to compromise it to change routes through systems we 'own,' then sniff from the owned DISA boxes," he said, describing a process of setting an invisible recorder to capture keystrokes or network traffic on a system.

But a system administrator with the Department of the Air Force said that the group's claims are overblown.

"So what if they stole a copy of the software that the [Department of Defense] uses to manage its networks. All that it shows is that the DOD has to pay millions to software companies for obscure software to manage its networks instead of buying off-the-shelf software like NT or Novell," said the sysadmin, who spoke on condition of anonymity.

"If it is just a simple tracking program that says 'this sub is going out over here,' then it's no big deal.... But if it had operational information like where the subs were, or where their missiles are targeted -- then that's something to be concerned about," the administrator said.

The MOD member said that he had been hacking for almost a decade, that he didn't worry about being caught, and that, as a hedge, he keeps all his private information cloaked with powerful 2048-bit encryption. Further, he said that he was browsing inside US Defense Department systems during the interview with Wired News.

The hacker confirmed earlier reports that MOD did not have hostile intentions, and he brushed off earlier comments that the group could sell the sensitive software.

"We spoke of selling it purely as an option to emphasize the DEM software's value when fully configured for operation with generated logs and reports, as the version we have comes with," he said.

"Our goals are to demonstrate the power of 15 or so individuals over large organizations, through publicizing break-ins and data retrieved," he said.

In February, US Attorney General Janet Reno announced that she would ask Congress for US$64 million to fund a new US center for fighting cybercrime. The National Infrastructure Protection Center would be a hub for a renewed counterattack on hackers around the world.

"Janet Reno needs to stand back and take a reality check," said the hacker.

"Any networked system cannot, and will not be entirely secure. It all depends how much of an element of 'human error' has been in the setup of the system through naiveté, etc.," he said.

As previously reported, the US Department of Defense says it keeps top-secret communications on a network called SIPRNET

that is physically disconnected from servers on the Internet.

But MOD says they have found that is not always the case.

"The administrative Naval Space Command systems are on the Internet and they contain a lot of 'interesting' data regarding weapons and communications technologies that are to be used by the DOD [including] energy weapons specifications," the hacker said.

But the Air Force systems administrator remained unimpressed by the group's threats of potential cyberwar.

"In the end, what does the theft of this software mean?" asked the administrator. "In the long run, not much. In the short term, the DOD will spend a few million to tighten up computer security even more."

"Does it affect the ability of the US military? Not at all.... even though the DOD likes to use computers, it's people and firepower that win wars. Computers only make the use of combat forces more effective," he said.

Editor's Note: Because of the anonymous nature of IRC, the real-world identity of the MOD member in this interview could not be confirmed.

Related Wired Links:

Have Crackers Found Military's Achilles' Heel?
21.Apr.98

Analyzer Headed for Army, Fame
31.Mar.98

Hacking Posse (Mostly) Leaves Web in Peace
27.Mar.98

Getting to the Bottom of 'Cyber Attacks'
26.Feb.98

Check on other Web coverage of this story with ***NewsBot***

Rants & Raves: Send your rants and raves to Wired News.

Tips: Have a story or tip for Wired News? Send it.

HOTWIRED

Copyright © 1993-97 Wired Ventures Inc. and affiliated companies.
All rights reserved.

TECHNOLOGY

GO

enter email

GO

Have Crackers Found Military's Achilles' Heel?

by James Glave

12:27pm 21.Apr.98.PDT

In what may be one of the first demonstrations of the potential of cyber warfare, an international cracking group claims it has stolen a suite of programs used to run classified US military networks and satellites.

The group, calling itself Masters of Downloading, or MOD, said in a statement that it had stolen the software -- the Defense Information Systems Network Equipment Manager (DEM) -- from the Defense Information Systems Agency, the branch of the Defense Department in charge of classified computer networks.

"This may help you to realize the reality of the threat of information warfare against the United States of America, as well as the DEM software's obvious value to certain global organizations and individuals," said the statement, which was supplied to Wired News by an anonymous representative of the group.

The statement detailed the capabilities of the DEM software, and was accompanied by a number of image files that depicted the program's interfaces. The software's authenticity was confirmed by John Vranesevich of the computer security site AntiOnline. Vranesevich said he obtained a copy from MOD last Thursday and tested it after first unplugging his computer from the Internet.

Vranesevich, who has tracked the computer underground for five years, said that the theft of a classified network control program pointed to a threat far more serious than the routine Web server intrusions of recent months.

"This is one of the first times we've seen a group of hackers whose goal was not to commit acts of Internet graffiti by defacing low-security Web pages, but [instead] to actually target, plan, and retrieve software suites designed for military use," said Vranesevich.

Last month, Vranesevich was the first to interview Ehud Tenebaum, the Israeli teen at the center of a federal investigation into widespread attacks on US military computer systems. But those attacks pale in comparison, he says.

"[The deliberate theft of classified software] puts this group on a whole other playing field," said Vranesevich, who added that the group is comprised of 15 individuals, including eight Americans, five Britons, and two Russians. The group is not affiliated with Tenebaum, known as the Analyzer.

MOD said that the software is used to remotely monitor and manage military computer-related

TECHNOLOGY
Today's Headlines

All-in-One DSL Modem Chips

Net Access via Apartment LANs

AntiOnline Founder Under Fire

Should Feds Trust Windows NT?

The Case of the Mistaken Spammer

OpenCable Progress Told

The Electronic Nose Knows

Networking Consumer Gadgets

Mining the Moon for Habitation

Small and Slow ... but Clean

Pumping Plastic

The Sound of Poison

equipment, including routers, repeaters, switches, military communication networks, and GPS satellites and receivers. The suite's top-level interface is designed to "manage all the computer-related equipment used by the United States military," the statement read.

With the DEM software, the group claims, the entire Defense Information Systems Network could be shut down for a period of time. "This is definitely not a good thing for the United States military, as they depend heavily on their computer systems and networks to quickly share data and information from anywhere in the world," the statement said.

MOD went into detail over two particular software components, one of which allows a user with access to monitor or shut down T1 links used by the military. The other program concerns Global Positioning System satellites, which are used to establish precise coordinates for weapons targeting and the navigation of commercial aircraft.

"Although the DEM software cannot be used to send data to the GPS satellites, it can be used to track the satellites and pinpoint their exact whereabouts, as well as the frequency ranges they use and other operational information," said the MOD statement.

MOD claims it first obtained the software in October 1997 but did nothing with it at first, to be sure that they were not being tracked.

Although the Defense Information Systems Agency public affairs office declined to comment, a mission statement on the agency's Web site clarifies its role within the Department of Defense: "DISA will be the preeminent provider of information systems delivery support to our warfighters and others as required by the DoD, under all conditions of Peace and War."

MOD members were not immediately available for comment, either, but in an interview with Vranesevich last Friday, group members said their intentions were not hostile.

"We have the power to do so, but at this time we have no intentions to launch such a [network] attack," a member told Vranesevich. Another member also told Vranesevich that he had obtained a separate piece of software used to communicate with submarines.

Gene Spafford, director of the Computer Security Research Center, COAST, said that the intrusion, if true, didn't surprise him.

"I don't think anyone who is familiar with government security has ever believed it to be as secure as claimed," Spafford said.

Spafford added that he was not familiar with DISA systems, but that any distributed system is vulnerable, and that many government systems

are configured "for convenience and not need."

The group claimed that they stole the software from a Windows NT server at DISA, and that about 30 individuals worldwide presently have copies.

"When you have a system that is distributed such that others can manipulate it, you open it up to not just security problems but also erroneous operations," Spafford said. "[You get] people who don't have training and [you get] accidents. It is a standard systems design question."

In an interview with Vranesevich, the group offered some network security advice for the US government.

"It's simple: take all [classified] military systems off the Internet, place only [unclassified] Web servers on the Internet [and] keep the rest on a purely internal network," the MOD member said.

Check on other Web coverage of this story with ***NewsBot***

Rants & Raves: Send your rants and raves to Wired News.

Tips: Have a story or tip for Wired News? Send it.

Copyright © 1993-97 Wired Ventures Inc. and affiliated companies.
All rights reserved.

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/01/1998

To: New York **Attn:** Financial Management Unit

From: New York
C-37
Contact: SA [redacted] ext.3187

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: UNSUBS a.k.a.
MASTERS OF DOWNLOADING, MOD;
DEFENSE INFORMATION SYSTEMS AGENCY
(DISA)-Victim
CITA
OO:NY

Synopsis: Request for confidential funds.

Details: Request $5,015 [redacted]

Previous Balance	$20,000.00
Requested Payment	$05,015.00
Balance	$14,985.00

♦♦

b3
b6
b7C
b7E

UPLOADED
WITH/TEXT ✓
WITH/ [redacted]
BY
DATE 6-8-98

[redacted]
SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
JUN 0 5 1998

er
Confund2.EC

b6
b7C

FAX COVER

Message:

Date : 4/16/98

[redacted]

You may already have this, but here is the information on the system where DEM was downloaded from.

[redacted]

[redacted]

b3
b6
b7C
b7E

To [redacted] New York FBI

Company :

Fax Number : 1-212-384-4660

From [redacted]

Company :

Fax Number : 1-703-494-8398

Pages including this cover page: 3

Subject : Insert Information

[redacted]

WinFax PRO Cover Page

 b6 b7C

[Query: sofie-tf.vgs.no, Server: whois.ripe.net]

% Rights restricted by copyright. See http://www.ripe.net/db/dbcopyright.html

domain:
descr:
admin-c:
tech-c:
zone-c:
nserver:
nserver:
notify:
changed:
changed:
changed:
changed:
changed:
changed:
source:

role:
address:
address:
address:
phone:
fax-no:
e-mail:
admin-c:
tech-c:
tech-c:
tech-c:
tech-c:
tech-c:
tech-c:
nic-hdl:
notify:
notify:
mnt-by:
changed:
changed:
changed:
source:

person:
address:
address:
address:
address:
phone:
fax-no:
e-mail:
nic-hdl:
notify:
changed:
source:

b6
b7C

b6
b7C

Record Request
FD-125 (Rev. 4-1-93)

Date 5-19-98

☐ Birth ☐ Credit ☒ Criminal ☐ Death ☐ INS ☐ Marriage* ☐ Motor Vehicle ☐ Other _____

To
OPC

Buded

Return
SA [redacted] C-37 ext 3187

File number [redacted]

b3
b6
b7C
b7E

Name and aliases of subject, applicant, or employee, and spouse
[redacted]

X [redacted]

Addresses
Residence
Business
Former

*Date and place of marriage (if applicable)

b3
b6
b7C
b7E

Race	Sex	Age	Height	Weight	Hair	Eyes
	☒ Male ☐ Female					

Birth date [redacted]
Birthplace
Arrest Number
Fingerprint classification
Criminal special [redacted]

Social Security Number
Drivers License Number
☐ D/L Photo ☐ Other

Specific information desired

Results of check

*Please call for pick up.

Thanks [redacted]

5/19/98

called 11:30 Am – 5/19/98 [redacted]

KFBI HINQ DCJS
10674 FILE 15 TYPE 1 NAME SEARCH TO DCJS (AND NCIC) PUR/C & F
.OPERATOR/.LOG/KFBI.CONFIDENTIAL LOG/N
.PUR/C.REASON/CRI.ORI/NYFBINY01.CASE#/[redacted]
.NAM/[redacted] .SEX/M.RAC/U.DOB/[redacted]
.SKIN TONE/*.HGT/* .SOC/* .FBI/* .MNU/*
.ALIAS#1/*
.ALIAS#2/*
.ALIAS#3/*
.ALIAS#4/*
.ALIAS#5/*
.REQUESTOR'S NAME[redacted]
.COMMENTS/CITA MATTERS

b3
b6
b7C
b7E

N 1121-1121 05/19/98 ROSQ# KFBI 08308 RDSQ# 03637095 PART 001 OF 001
NYSP PTST KFBI 1122
NYFBINY01
NO [redacted] WANTED PERSONS FILE
NAM[redacted]
.DOB/[redacted] SEX/M.RAC/U

N 1121-1121 05/19/98 ROSQ# KFBI 08309 RDSQ# 03637113 PART 001 OF 001
NCIC PTST KFBI 1122
NYFBINY01

MKE/MISSING PERSON [redacted]
ORI/CA0300000 NAM[redacted] SEX/M RAC/W DOB[redacted]
DOE/[redacted] HGT[redacted] WGT/[redacted] EYE[redacted] HAI/[redacted] SKN[redacted]
MNP/MP DLC/120497 OCA/9764086
MIS/SOUTH INV
ORI IS ORANGE CO SO SANTA ANA CA
NIC/M081029107
IMMED CONFIRM MISSING PERSON STATUS WITH ORI

b6
b7C

N 1121-1122 05/19/98 ROSQ# KFBI 08310 RDSQ# 03637144 PART 001 OF 001
NCIC HINQ KFBI
ACK
NYFBINY01
NO IDENTIFIABLE RECORD IN THE INTERSTATE IDENTIFICATION INDEX (III)
FOR NAM[redacted]SEX/M.RAC/U.D0B/[redacted]PUR/C.
END

b6
b7C

N 1121-1122 05/19/98 ROSQ# KFBI 08311 RDSQ# 03637212 PART 001 OF 001
NYIS HINQ KFBI 1122
KFBI10674 NO SUSPECTS

Record Request
FD-125 (Rev. 4-1-93)

Please [redacted] on the driver info for [redacted] the following 6 vehicles. Please see attached sheet. Thank You. Dieter

Date 5-19-98

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☒ Motor Vehicle ☐ Other

To OPC

Buded

Return to SA [redacted] C-37 ext. 3187

F [redacted]

b3
b6
b7C
b7E

Name and aliases of subject, applicant, or employee, and spouse

[redacted] X [redacted]

Addresses

Residence

Business

Former

*Date and place of marriage (if applicable)

Race	Sex	Age	Height	Weight	Hair	Eyes
	☒ Male ☐ Female					

Birth date | Birthplace

Arrest Number | Fingerprint classification | Criminal specialty

Social Security Number | Drivers License Number

☐ D/L Photo ☐ Other

Specific information desired

Results of check

[redacted]

b3
b6
b7C
b7E

* Please call for [redacted] Pick-up. 5.19.98

Thanks. Dieter

[redacted]

N 1659-1659 05/18/98 ROSQ# KFBI 07641 RDSQ# 02118920 PART 001 OF 001
LETS KFBI
23945 AM CA0340700 13787 NYFBINY01 11413 14:03-14:03 05/18/98
TXT
AUTH SA [redacted] C37 [redacted]

b6
b7C

FIND FOLLOWING TO [redacted]
LIC [redacted] SUZI OF VISALIA
LIC [redacted] FORD
LIC [redacted] VESSEL
LIC [redacted] CHEV
LIC [redacted] CHEV
LIC [redacted] FORD

Please run driver info for these.

RE MSG DATE
DEPT OF MOTOR VEHICLES SACRAMENTO CALIF MM

KFBI RVEH LETS
.NYFBINY01.CA,* ,* ,* ,* .
LIC/[redacted].LIY/98.LIT/PC.
MIS/SA[redacted]C37

N 1116-1116 05/19/98 ROSQ# KFBI 08286 RDSQ# 03618120 PART 001 OF 001
NYSP TTST KFBI 1116
NYFBINY01
NO RECORD NYSPIN LIC[redacted].CA

b6
b7C

N 1116-1116 05/19/98 ROSQ# KFBI 08287 RDSQ# 03618132 PART 001 OF 001
NCIC TTST KFBI 1116
NYFBINY01
NO RECORD LIC/[redacted]LIS/CA

N 1116-1116 05/19/98 ROSQ# KFBI 08288 RDSQ# 03618707 PART 001 OF 001
LETS KFBI
35788 RR CALIC0000 05562 NYFBINY01 05662 08:19-08:19 05/19/98
*KFBI00RVEH
TXT
DATE: 05/19/98 TIME: 08:16
REG VALID FROM: 02/02/96 TO 02/02/97
LIC#[redacted]YRMD:88 MAKE:SUZI BTM :CV VIN :JS4JC51C3J4226400
RCID:05/08/96 REC STATUS:
OPEN COLL ACCT

b6
b7C

END

KFBI RVEH LETS
.NYFBINY01.CA,* ,* ,* ,* .
LIC[redacted].LIY/98.LIT/PC.
MIS/SA[redacted]C37

N 1116-1116 05/19/98 ROSQ# KFBI 08289 RDSQ# 03619123 PART 001 OF 001
NYSP TTST KFBI 1116
NYFBINY01
NO RECORD NYSPIN LIC[redacted]CA

b6
b7C

N 1116-1116 05/19/98 ROSQ# KFBI 08290 RDSQ# 03619160 PART 001 OF 001
NCIC TTST KFBI 1116
NYFBINY01
NO RECORD LIC/[redacted]LIS/CA

N 1116-1116 05/19/98 ROSQ# KFBI 08291 RDSQ# 03619856 PART 001 OF 001
LETS KFBI
35798 RR CALIC0000 05568 NYFBINY01 05672 08:19-08:19 05/19/98
*KFBI00RVEH
TXT
DATE: 05/19/98 TIME: 08:17
PNO VALID FROM: 05/22/97
REG VALID FROM: 06/02/96 TO 06/02/97
LIC#:[redacted] YRMD:63 MAKE:FORD BTM :SD VIN :3R01U168425
R/O [redacted] CITY:[redacted]
C.C.:54 ZIP#:[redacted]
SOLD:00/00/63 RCID:05/29/96 OCID:11/12/92 LOCD:9

b6
b7C

PNO-REGISTRATION DEFERRED

11/02/92 PREV LIC [redacted]

END

KFBI RVEH LETS
.NYFBINY01 CA,* ,* ,* ,* .
LIC/[redacted] .LIY/98.LIT/PC.
MIS/SA[redacted] C37

N 1116-1116 05/19/98 ROSQ# KFBI 08292 RDSQ# 03620325 PART 001 OF 001 b6 b7C
NYSP TTST KFBI 1116
NYFBINY01
NO RECORD NYSPIN LIC[redacted] CA

N 1116-1116 05/19/98 ROSQ# KFBI 08293 RDSQ# 03620333 PART 001 OF 001
NCIC TTST KFBI 1116
NYFBINY01
NO RECORD LIC/[redacted] LIS/CA b6 b7C

KFBI RVEH LETS
.NYFBINY01 CA,* ,* ,* ,* .
LIC[redacted] .LIY/98.LIT/PC. b6 b7C
MIS/SA[redacted] C37

N 1116-1116 05/19/98 ROSQ# KFBI 08294 RDSQ# 03620858 PART 001 OF 001
NYSP TTST KFBI 1116
NYFBINY01
NO RECORD NYSPIN LIC/[redacted] CA b6 b7C

N 1116-1116 05/19/98 ROSQ# KFBI 08295 RDSQ# 03620872 PART 001 OF 001
NCIC TTST KFBI 1116
NYFBINY01
NO RECORD LIC/[redacted] LIS/CA

N 1116-1116 05/19/98 ROSQ# KFBI 08296 RDSQ# 03620987 PART 001 OF 001
LETS KFBI
35804 RR CALIC0000 05577 NYFBINY01 05678 08:20-08:20 05/19/98
*KFBI00RVEH
TXT
DATE: 05/19/98 TIME: 08:17
[redacted]-RECORD NOT ON FILE

END

N 1116-1117 05/19/98 ROSQ# KFBI 08297 RDSQ# 03621400 PART 001 OF 001
LETS KFBI
35807 RR CALIC0000 05579 NYFBINY01 05680 08:20-08:20 05/19/98
*KFBI00RVEH
TXT
DATE: 05/19/98 TIME: 08:17
REG VALID FROM: 05/20/97 TO 05/20/98
LIC#: [redacted] YRMD:74 MAKE:CHEV BTM :SD VIN :1L39L4C146400
R/O #[redacted]
[redacted] CITY:[redacted] C.C.:54 ZIP#:[redacted]
SOLD:00/00/74 RCID:05/05/97 OCID:05/15/97 LOCD:3

07/06/78 PREV LIC 650823

01/11/1997-ODOMETER: 134,413 MILES ACTUAL MILEAGE

END

b6
b7C

KFBI RVEH LETS
.NYFBINY01.CA,* ,* ,* ,* .
LIC/[redacted] .IIY/98.LIT/PC.
MIS/SA [redacted] C37

b6
b7C

N 1117-1117 05/19/98 ROSQ# KFBI 08298 RDSQ# 03622108 PART 001 OF 001
NYSP TTST KFBI 1117
NYFBINY01
NO RECORD NYSPIN LIC/[redacted] CA

N 1117-1117 05/19/98 ROSQ# KFBI 08299 RDSQ# 03622118 PART 001 OF 001
NCIC TTST KFBI 1117
NYFBINY01
NO RECORD LIC/ [redacted] LIS/CA

b6
b7C

N 1117-1117 05/19/98 ROSQ# KFBI 08300 RDSQ# 03622469 PART 001 OF 001
LETS KFBI
35813 RR CALIC0000 05585 NYFBINY01 05687 08:20-08:20 05/19/98
*KFBI00RVEH
TXT
DATE: 05/19/98 TIME: 08:17
REG VALID FROM: 11/14/97 TO 11/14/98
LIC#: [redacted] YRMD:80 MAKE:CHEV BTM :SD VIN :1X687A6138407
R/O [redacted] C88 CITY: [redacted]
C.C.:54 ZIP#: [redacted]
SOLD:00/00/79 RCID:01/29/98 OCID:02/08/98 LOCD:3

b6
b7C

END

KFBI RVEH LETS
.NYFBINY01.CA,* ,* ,* ,* .
LIC/NFR713 .LIY/98.LIT/PC.
MIS/SA [redacted] C37

b6
b7C

N 1117-1117 05/19/98 ROSQ# KFBI 08301 RDSQ# 03623693 PART 001 OF 001
NYSP TTST KFBI 1117
NYFBINY01
NO RECORD NYSPIN LIC/ [redacted] CA

N 1117-1117 05/19/98 ROSQ# KFBI 08302 RDSQ# 03623733 PART 001 OF 001
NCIC TTST KFBI 1117
NYFBINY01
NO RECORD LIC/ [redacted] LIS/CA

b6
b7C

N 1117-1117 05/19/98 ROSQ# KFBI 08303 RDSQ# 03624092 PART 001 OF 001
LETS KFBI
35825 RR CALIC0000 05599 NYFBINY01 05699 08:20-08:20 05/19/98
*KFBI00RVEH
TXT
DATE: 05/19/98 TIME: 08:18
REG VALID FROM: 06/12/91 TO 06/12/92
LIC#: [redacted] YRMD:65 MAKE:FORD BTM :SED07 VIN :5R07A201729
R/O [redacted] CITY: [redacted] C.C.:54 ZIP#: [redacted]
SOLD:00/00/65 RCID:06/05/91 OCID:09/09/87 LOCD:9

END

KFBI RVEH LETS
.NYFBINY01.CA,* ,* ,* ,* .
LIC [redacted] .LIY/98.LIT/PC.
MIS/SA [redacted] C37

b6
b7C

N 1118-1118 05/19/98 ROSQ# KFBI 08304 RDSQ# 03625802 PART 001 OF 001
NYSP TTST KFBI 1118
NYFBINY01
NO RECORD NYSPIN LIC [redacted]

N 1118-1118 05/19/98 ROSQ# KFBI 08305 RDSQ# 03626190 PART 001 OF 001
NCIC TTST KFBI 1118
NYFBINY01
NO RECORD LIC/ [redacted] LIS/CA

b6
b7C

N 1118-1118 05/19/98 ROSQ# KFBI 08306 RDSQ# 03626563 PART 001 OF 001
LETS KFBI
35839 RR CALIC0000 05607 NYFBINY01 05712 08:21-08:21 05/19/98
*KFBI00RVEH
TXT
DATE: 05/19/98 TIME: 08:19
[redacted] RECORD NOT ON FILE

b6
b7C

END

KFBI BVEH LETS
.NYFBINY01.CA.* ,* ,* ,* .
REG [redacted]
MIS/SA [redacted] C37

N 1120-1120 05/19/98 ROSQ# KFBI 08307 RDSQ# 03633962 PART 001 OF 001
LETS KFBI
35896 BR CABOAT000 05665 NYFBINY01 05770 08:24-08:24 05/19/98
*KFBI00BVEH
TXT
DATE: 05/19/98 TIME: 08:21
REG VALID FROM: 12/31/97 TO 12/31/99
LIC#: [redacted] YRMD:61 MAKE:TROJAN BTM :VESSEL VIN :CFZ9541H0000T
R/O [redacted]
[redacted] CITY: [redacted] C.C.:54 ZIP#: [redacted]
SOLD:09/21/96 RCID:12/31/97 OCID:11/29/96 LOCD:3

HULM:W PRPL:I FEET:024 INCH:01

END

b6
b7C

Record Request
FD-125 (Rev. 4-1-93)

Date 5-18-98

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☒ Motor Vehicle ☐ Other

To OPC	Buded
Return to SA [redacted] -37 ext 3187	File number [redacted]

b3 b6 b7C b7E

Name and aliases of subject, applicant, or employee, and spouse [redacted] (X) [redacted]

Addresses
Residence California
Business
Former

*Date and place of marriage (if applicable)

Race	Sex	Age	Height	Weight	Hair	Eyes
	☒ Male ☐ Female					

Birth date	Birthplace	
Arrest Number	Fingerprint classification	Criminal specialty
Social Security Number	Drivers License Number ☐ D/L Photo ☐ Other	

Specific information desired

b3 b6 b7C b7E

Results of check [redacted]

Please call for pick-up. [redacted] -3187

[redacted] JUN 1 / 1998 [redacted]

KFBI FL25 LETS
AM.NYFBINY01.CAOLN0000.
10456 FILE 25 FBI NEW YORK OFFICE NYFBINY01 MAY 18-98
TO CA DMV

NEED ALL DRIVERSLICENSE AND VEHICLES REG TO [redacted] THE CASE AGENT DOESN'T HAVE ANY OTHER INFORMATION.

b6
b7C

AUTH SA [redacted] C37 [redacted] 11-40 AM

Record Request
FD-125 (Rev. 4-1-93)

CA ←

Date 6-16-98

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☒ Motor Vehicle ☐ Other _____

Driver Id Info

To OPC

Buded

Return to SA [redacted] C-37 ext 3187

File number [redacted]

b3
b6
b7C
b7E

Name and aliases of subject, applicant, or employee, and spouse

[redacted]

License ID [redacted]

1,4 [redacted]

Addresses

Residence

Business

Former

*Date and place of marriage (if applicable)

Race	Sex	Age	Height	Weight	Hair	Eyes
	☒ Male ☐ Female					

Birth date

Birthplace

Arrest Number

Fingerprint classification

Criminal specialty

Social Security Number

Drivers License Number [redacted]

☐ D/L Photo ☐ Other

b3
b6
b7C
b7E

Specific information desired [redacted]

Results of check

Please call for pick-up.

[redacted] 6/16

[redacted] -3187

[redacted]

KFBI DLIC LETS
.NYFBINY01.CA.
OLN/B7458092
MIS/SA [redacted] C37

N 1348-1348 06/16/98 RDSQ# KFBI 31086 RDSQ# 01855660 PART 001 OF 001
LETS KFBI
13722 DR CAOLN0000 09462 NYFBINY01 09523 10:52-10:52 06/16/98
*KFBI00DLIC
TXT
NAME [redacted]
ADDR [redacted]

SEX/M. DOB [redacted] HGT/506. WGT/135. HAI/BRO. EYE/BLU.

OLN/ [redacted] EXP [redacted] /99

RSTR:PROVISIONAL LICENSEE

STATUS:VALID

END

b6
b7C

Record Request
FD-125 (Rev. 4-1-93)

Date 6-16-98

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☒ Motor Vehicle ☐ Other _____

To
OPC

Buded

Return to
SA [redacted]

File number [redacted]

b3
b6
b7C
b7E

Name and aliases of subject, applicant, or employee, and spouse
CALIFORNIA LICENSE PLATE
1ZZB856

Addresses
Residence
Business
Former

*Date and place of marriage (if applicable)

Race	Sex	Age	Height	Weight	Hair	Eyes
	☐ Male ☐ Female					

Birth date | Birthplace

Arrest Number | Fingerprint classification | Criminal specialty

Social Security Number | Drivers License Number

☐ D/L Photo ☐ Other

Specific information desired

b3
b6
b6
b7C
b7E

Results of check

Please call for pick-up

Thanks. [redacted] - 3187

[redacted]
6/16

[redacted]

FMT RVEH LEYS

KFBI RVEH LETS
.NYFBINY01.CA,* ,* ,* ,* .
LIC/1ZZB856 .LIY/98.LIT/PC.
MIS/SA [redacted] C37

N 1354-1354 06/16/98 RDSQ# KFBI 31091 RDSQ# 01871133 PART 001 OF 001
NYSP TTST KFBI 1354
NYFBINY01
NO RECORD NYSPIN LIC/1ZZB856.CA

b6
b7C

N 1354-1354 06/16/98 RDSQ# KFBI 31092 RDSQ# 01871163 PART 001 OF 001
NCIC TTST KFBI 1354
NYFBINY01
NO RECORD LIC/ 1ZZB856 LIS/CA

N 1355-1355 06/16/98 ROSQ# KFBI 31093 RDSQ# 01871998 PART 001 OF 001
LETS KFBI
13928 RR   CALIC0000 09611 NYFBINY01 09729 10:58-10:59 06/16/98
*KFBI00RVEH
TXT
DATE: 06/16/98 TIME: 10:55
REG VALID FROM: 03/31/98 TO 03/31/99
LIC#:1ZZB856 YRMD:94 MAKE:LINC BTM :LM VIN :1LNLM81W4RY721984
R/O :FLEETWOOD LIMOUSINSE LTD, 5855 GREEN VALLEY CIR, STE 107
CITY:CULVER CITY C.C.:19 ZIP#:90230
SOLD:00/00/94 RCID:04/11/98 OCID:01/01/97 LOCD:3

12/20/96 PREV LIC   5E13114

08/20/1996--ODOMETER: 43,080 MILES ACTUAL MILEAGE

END

Record Request
FD-125 (Rev. 4-1-93)

Date 5-18-98

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☒ Motor Vehicle ☐ Other

To
ODL

Buded

Return to
SA [redacted] C-37 ext 3187

File number [redacted]

b3
b6
b7C
b7E

Name and aliases of subject, applicant, or employee, and spouse
[redacted]

[redacted]

Addresses
Residence CALIFORNIA

Business

Former

*Date and place of marriage (if applicable)

Race	Sex	Age	Height	Weight	Hair	Eyes
	☒ Male ☐ Female					

Birth date | Birthplace

Arrest Number | Fingerprint classification | Criminal specialty

b3
b6
b7C
b7E

Social Security Number | Drivers License Number

☐ D/L Photo ☐ Other [redacted]

Specific information desired

Results of check [redacted]

5/18/98

Please call for pick-up.

[redacted] -3187

[redacted]

KFBI FL25 LETS
AM. NYFBINY01. CAOLN0000.
10453 FILE 25 FBI NEW YORK OFFICE NYFBINY01 MAY 18-98
TO CA DMV

NEED ALL DRIVERS LICENSE AND VEHICLES REG TO [redacted] CASE AGENT HAS NO OTHER INFORMATION.

b6
b7C

AUTH SA [redacted] C37 [redacted] 11-37AM

N 1654-1654 05/18/98 ROSQ# KFBI 07634 RDSQ# 02108473 PART 001 OF 001
LETS KFBI
23858 AM CA0340770 13663 NYFBINY01 11327 13:57-13:57 05/18/98
TXT
001 CALIF DDL
FBI NEW YORK
AUTH SA [redacted] C37

RE [redacted] DOB [redacted] CDL# [redacted]

b6
b7C

N 1658-1658 05/18/98 ROSQ# KFBI 07637 RDSQ# 02115850 PART 001 OF 001
LETS KFBI
23917 DR   CAOLN0000 13753 NYFBINY01 11386 14:01-14:01 05/18/98
*KFBI00DLIC
TXT
MATCHED ON:*L/N*F/N* BD

NAME [redacted]
ADDR

SEX/M. DOB/[redacted] HGT/504. WGT/115. HAI/BLN. EYE/BLU.

OLN [redacted] EXP [redacted]00

RSTR:NONE

STATUS:NO VALID OLN

END

b6
b7C

KFBI DLIC LETS
.NYFBINY01.CA.* .* ,* ,* .
NAM[redacted] .DOB[redacted] SEX/M.
MIS/SA [redacted] C37

N 1658-1658 05/18/98 ROSQ# KFBI 07635 RDSQ# 02115712 PART 001 OF 001
NYSP PTST KFBI 1658
NYFBINY01
NO RECORD - NYSPIN WANTED PERSONS FILE
NAM[redacted]
.DOB[redacted] SEX/M.RAC/U

b6
b7C

N 1658-1658 05/18/98 ROSQ# KFBI 07636 RDSQ# 02115724 PART 001 OF 001
NCIC PTST KFBI 1658
NYFBINY01

MKE/MISSING PERSON - JUVENILE
ORI/CA0300000 NAM/[redacted] SEX/M RAC/W DOB[redacted]
DOE/112898 HGT/505 WGT/115 EYE/BLU HAI/BR0 SKN/LGT
MNP/MP DLC/120497 OCA/9764086
MIS/S0UTH INV
ORI IS ORANGE CO SO SANTA ANA CA
NIC[redacted]
IMMED CONFIRM MISSING PERSON STATUS WITH ORI

b6
b7C

N 1701-1701 05/18/98 ROSQ# KFBI 07642 RDSQ# 02121551 PART 001 OF 001
LETS KFBI
23962 AM CA0340700 13816 NYFBINY01 11431 14:04-14:04 05/18/98
TXT
AUTH SA [redacted] C37 [redacted]

FIND NO VEHICLE REG TO [redacted] AS GIVEN

b6
b7C

RE MSG DATE
DEPT OF MOTOR VEHICLES SACRAMENTO CALIF MM

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/01/1998

On May 13, 1998, Special Agents of the Federal Bureau of Investigation conducted a surveillance in the vicinity if 18124 Culver Drive, Irvine, California. Photographic Specialist [redacted] was also present and took photographs. The following observations were made: b6 b7C

2:15 PM Surveillance initiated.

3:53 PM Blue four door Lincoln Town Car limousine bearing California license 1ZZB856 observed entering the parking lot at the Shepard of Grace Lutheran Church, 18182 Culver Drive. The driver reclined his seat after parking the vehicle.

4:12 PM Limousine departed the parking lot and relocated to the parking lot to the east of the dental clinic at 18124 Culver Drive.

4:16 PM Two white males approximately 17- 19 years of age wearing black trench coats observed in the parking lot walking towards the limousine. One of the males appeared to be carrying a yellow telephone linesman's handset. Both males entered the limousine. b6 b7C

4:19 PM The limousine departed on Culver Drive and headed towards the 405 freeway.

4:20 PM Surveillance discontinued.

[redacted] b3 b6 b7C b7E

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
JUL [redacted] 1998
FBI [redacted]

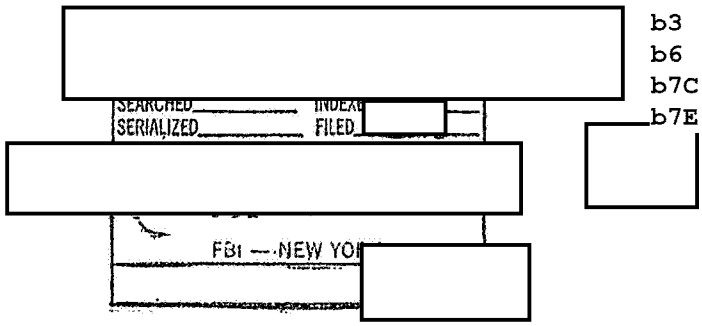
Investigation on 05/13/1998 at Irvine, California

File # [redacted] Date dictated [redacted]

by SA [redacted] SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b3
b6
b7C
b7E



b3
b6
b7C
b7E

The following investigation was conducted, by Special Agent [redacted] at Irvine, California:

The following cars were observed on 5/13/98, at 10:55 p.m., parked in the public parking lot between University Park Medical Dental Center, 18124 Culver and Rite Aid, 18112 Culver:

[redacted]

CA Nissan XE pickup, white
CA Ford Discovery van, brown and tan
CA Jaguar 2-door, red
CA Plymouth Spirit LE 4-door, white
CA 4-door, black
CA
CA 2-door
CA Nissan Sentra 4-door
CA 4-door, blue
CA Mazda 626 4-door, silver
CA Ford Thunderbird 2-door, white

b3
b6
b7C
b7E

[redacted]

The following cars were observed on 5/13/98 at 10:55 p.m., parked in the public parking lot between Carls Jr., 18032 Culver and Tacos & Company:

[redacted]

CA Toyota 2-door, silver
CA Ford pickup, brown and tan
CA dist (blue and gold plate) Hyundai 2-door
CA Dodge van, blue
CA Lexus 4-door, white
CA Jeep 2-door
CA Ford pickup, white
CA van
Chevrolet Z71 pickup
CA dist (blue and white plate) 2-door, silver
CA Volvo 740 GL station wagon
CA Honda 4-door, white

b6
b7C

none

[redacted]

The following cars were observed on 5/14/98, at 6:19 a.m., parked in the public parking lot between University Park Medical Dental Center, 18124 Culver and Rite Aid, 18112 Culver:

[redacted]

CA Nissan XE pickup, white

b3
b6
b7C
b7E

[redacted]

CA Ford Discovery van, brown and tan
CA Plymouth Spirit LE 4-door, white
CA Mazda 626 4-door, silver
CA Honda 4-door, black
CA Mercedes Benz S600 2-door black
CA Ford ambulance, white

The following cars were observed on 5/14/98 at 6:19 a.m., parked in the public parking lot between Carls Jr., 18032 Culver and Tacos & Company:

[redacted]

CA Honda Accord 4-door, green
CA Toyota 4-door, tan
CA Ford van
CA Ford pickup, blue
CA Mercedes Benz 4-door, black
CA Honda 4-door, silver
CA van, gray
CA Ford Contour 4-door, white
CA Ford 2-door, white
CA Chevrolet 4-door, blue
CA Ford F-250 pickup, white
CA Toyota Supra 2-door, blue
CA Chevrolet 4-door, white

b6
b7C

The white Nissan XE pickup license [redacted] and the brown and tan Ford Discovery van license [redacted] were parked one stall apart, directly behind the University Park Medical Dental Center buildings. A walk past each of the vehicles revealed a set of automotive fuses on the driver's seat of the Nissan pickup and nothing visible in the Ford van. The ground was dry under both vehicles, whereas the rest of the area was wet from rainfall. A Carl's Jr. cup sat atop the left rear tire of the Nissan pickup.

The white Plymouth Spirit license [redacted] was parked immediately fronting Rite Aid.

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/01/1998

To: New York **Attn:** SA [redacted]
Squad C-37

From: Los Angeles
WCC-3
Contact: SA [redacted] 310-996-3962

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending) -32

b3
b6
b7C
b7E

Title: UNSUBS aka
MASTERS OF DOWNLOADING (MOD);
DEFENSE INFORMATION SYSTEMS AGENCY-
(DISA) -VICTIM;
CITA
OO:NY

Synopsis: Surveillance photographs of MOD UNSUBS obtained by Los Angeles and enclosed for New York. Lead covered in Los Angeles.

Reference: [redacted]

Administrative: Telcalls between SA [redacted] and SA [redacted]

Enclosures:
1. Insert re surveillance at Irvine, CA.
2. FD-302 surveillance log from 05/13/98, Irvine, CA.
3. 1A envelope containing original notes for enclosure 2.
4. 1A envelope containing surveillance photographs.

b3
b6
b7C
b7E

Details: Referenced serial set a lead for Los Angeles to obtain photographs of members of a group called MASTERS OF DOWNLOADING or MOD.

On 05/13/1998 WCC-3 agents successfully accomplished a discrete surveillance of two members of MOD in the vicinity of 18124 Culver Drive, Irvine, California. An FD-302 containing the surveillance log is enclosed along with photographs of two male subjects. The enclosed insert lists the automobiles present at the pick up location later on the night of 05/13/1998.

The two young males arrived at the location presumably by vehicle and were transported via limousine to an unknown

SEARCHED INDEXED
SERIALIZED FILED
JUN 18 1998
YORK

b3
b7E

location, just as New York had advised would happen. Agents did not observe the subjects arriving in a vehicle; the subject's were walking in the parking lot when first observed. No efforts were made to follow the limo per instructions from SA [redacted] in New York. Los Angeles was informed on 05/14/1998 by SA [redacted] that the subjects did not leave a vehicle in the parking lot overnight, so the enclosed insert will be of no investigative value but is provided to New York never-the-less.

For the information of New York, the limo discussed above was found to be registered to Fleetwood Limousine LTD, 5855 Green Valley Circle, Suite 107, Culver City, California. Additionally at the request of SA [redacted] local files were checked for the name [redacted] DOB [redacted] Missing person records indicate that [redacted] is a juvenile runaway from Orange County, California.

b6
b7C

Los Angeles is standing by if further assistance is required. Lead covered.

♦♦

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/08/98

On 04/22/98 thru 04/29/98 [redacted] provided the following information to Special Agent [redacted] of the New York office of the FEDERAL BUREAU OF INVESTIGATION (FBI):

[redacted] learned from a MASTERS OF DOWNLOADING (MOD) member that the MOD [redacted]

b6
b7C
b7D
b7E

File = 0429.302

[redacted]

Investigation on 04/22-29/98 at New York, NY

File # [redacted] Date dictated 06/08/98

by SA [redacted]

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
JUN 1 1 1998
FBI - NY

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UPLOADED
WITH/TEXT ✓
WITH/OUT TEXT
BY [redacted]
DATE 10-19-98

b6
b7C

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/09/98

SOURCE, who is not in a position to testify, provided the following information:

[redacted]

b6
b7C
b7D
b7E

File: 0503-[redacted].302

Investigation on 05/03/-05/11/98 New York, NY

File # [redacted] Date dictated 06/09/9[redacted]

by SA [redacted]

b3
b6
b7C
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UPLOADED

WITH ATT ✓

WITHOUT ATT

BY [redacted]

DATE 10-19-98

b6
b7C

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 06/01/1998

To: New York Attn: Financial Management Unit

From: New York
C-37
Contact: SA [redacted] ext.3187

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: UNSUBS a.k.a.
MASTERS OF DOWNLOADING, MOD;
DEFENSE INFORMATION SYSTEMS AGENCY
(DISA)-Victim
CITA
OO:NY

Synopsis: Request for confidential funds.

Details: [redacted]

b3
b6
b7C
b7E

♦♦

File POBOX. EC

[redacted]

SERIALIZ[redacted]

UPLOADED
WITH[redacted]
[redacted]
BY [redacted]
DATE 6-19-98

Record Request
FD-125 (Rev. 4-1-93)

Date 6-19-98

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☐ Motor Vehicle ☐ Other _____

To OPC | Buded

Return to SA [redacted] C37 ext. 3187 | [redacted]

b3
b6
b7C
b7E

[redacted] plicant, or employee, and spouse

[redacted]

Addresses
Residence
Business
Former

*Date and place of marriage (if applicable)

Race	Sex	Age	Height	Weight	Hair	Eyes
	☒ Male ☐ Female					

Birth date [redacted] | Birthplace [redacted]

b3
b6
b7C
b7E

Arrest Number | Fingerprint classification | Criminal specialty

Social Security Number [redacted]

Drivers License Number

☐ D/L Photo ☐ Other

Specific information desired [redacted]

Results of check

[redacted]

JUN 22 1998

FBI - NEW YORK

[redacted]

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/17/98

[redacted] U.S. POSTAL INSPECTOR, New York Office, telephone number [redacted] was interviewed telephonically. After being advised of the identity of the interviewing agent and the nature of the interview, he provided the following information: b6 b7C [redacted]

[redacted] was rented by [redacted]

[redacted]

Investigation on 05/20/98 at New York, NY

File # [redacted] Date dictated 06/17/98

by SA [redacted]

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
Telephonic
JUN 22 1998
FBI — NEW YORK

b3 b6 b7C b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

[redacted]
302

UPLOADED

WITH/T XT ✓

WIT /O

BY

DATE 6-24-98

b6
b7C

Record Request
FD-125 (Rev. 4-1-93)

Date 6-19-98

☐ Birth ☐ Credit ☐ Criminal ☐ Death ☐ INS ☐ Marriage* ☐ Motor Vehicle ☐ Other _____

To	Buded
OPC	
Return to [redacted] C-31	File number [redacted]

b3 b6 b7C b7E

Name and aliases of subject, applicant, or employee, and spouse

[redacted] 1 [redacted]

Addresses

Residence _____

Business _____

Former _____

*Date and place of marriage (if applicable) _____

Race	Sex	Age	Height	Weight	Hair	Eyes
	☒ Male ☐ Female					

Birth date	Birthplace
[redacted]	

Arrest Number	Fingerprint classification	Criminal specialty

Social Security Number [redacted]

Drivers License Number [redacted]

☐ D/L Photo ☐ Other

b3 b6 b7C b7E

Specific information desired [redacted]

Results of check

[redacted]

[redacted]

SEARCHED INDEXED
SERIALIZED FILED
JUN 23 1998
FBI — NEW YORK

[redacted]

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/15/1998

To: New York

From: New York
C-37
Contact: SA [redacted] ext.3187

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: "CHANGED";
[redacted]
a.k.a. [redacted];
[redacted]
a.k.a. [redacted]
a.k.a. MASTERS OF DOWNLOADING;
DEFENSE INFORMATION SYSTEM AGENCY
(DISA)-VICTIM;
CITA;
OO:NY

Synopsis: Title "CHANGED" to identify subject.

Previous Title: UNSUBS a.k.a.
MASTERS OF DOWNLOADING;
DEFENSE INFORMATION SYSTEM AGENCY
(DISA) - VICTIM;
CITA;
OO:NY

Details: Title marked "CHANGED" to reflect the subject identified.

♦♦

File - title_ch.ec

[redacted]

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
JUN 2 [illegible] 1998
FBI — NEW YORK
[redacted]

b3 b6 b7C b7E

UPLOADED
WITH/TEXT ✓
WITHOUT TEXT
BY [redacted]
DATE 6-29-98

title changed 6-30-98

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/15/98

SOURCE, who is not in a position to testify, provided the following information:

[redacted]

b6
b7C
b7D
b7E

[redacted]

b3
b6
b7C
b7E

0514_21.302

Investigation on 05/14 - 21/98 at New York, NY

File # [redacted]

Date dictated 06/15/98

by SA [redacted]

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
JUN 23 1998
FBI — NEW YORK

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UPLOADED

WITH/TT ✓

WIT

BY [redacted]

DA 6-29-98

b6
b7C

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/29/1998

To: Los Angeles **Attn:** SSA [redacted] b3 b6 b7C b7E

From: New York
C-37
Contact: SA [redacted] 212-384-3187

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: [redacted]
a.k.a. [redacted] SN|PER;
[redacted]
a.k.a. [redacted]
a.k.a . MASTERS OF DOWNLOADING;
DEFENSE INFORMATION SYSTEM AGENCY
(DISA) - VICTIM
CITA
OO:NY

Synopsis: Set lead for Los Angeles to return search warrant results to United States District Court, Central District of California.

Enclosures: 1) 1 - Original Search Warrant for [redacted]

2) 8 - Original FD-597s Receipt for Property Seized Forms for [redacted]

3) 1 - Copy of Search Warrant for [redacted] b6 b7C

4) 8 - Copied FD-597s Receipt for Property Seized Forms for [redacted]

Details: On 06/26/98, a search warrant was executed on [redacted] SA [redacted] was unable to return the results of the search warrant before returning to New York.

[redacted] b3 b6 b7C b7E

4053 7951 4299 FedEx 30 Jun 98
SEARCHED SERIALIZED FILED
JUL - 2 19[redacted]

06291cad.ec

UPLOADED
WITH TEXT
WITHOUT TEXT
BY
DATE 7-10-98

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/17/98

Col. [redacted] and Lt. [redacted] DISA, telephone number [redacted] were interviewed telephonically. After being advised of the identity of the interviewing agent and the nature of the interview, they provided the following information:

b6
b7C

The DEM software is unclassified software. DEM was not widely distributed or available publicly. DEM allows DEFENSE INFORMATION SYSTEMS AGENCY (DISA) system administrators to remotely configure parts of the DISA computer networks. DEM is located on four servers around the world. An unauthorized user of DEM could turn off multiplexers and 1/6 of telephone/data connections on parts of the DISA network.

DISA network topology maps were distributed widely and made publicly over the Internet at *.LES.mil.

COL - [redacted] 302

[redacted]

b3
b6
b7C
b7E

Investigation on 05/26/98 at New York, NY (telephonically)

File [redacted] Date dictated 06/17/98

by SA [redacted]

SEARCHED [redacted] INDEXED [redacted]
SERIALIZED [redacted] FILED [redacted]
JUN 22 1998
FBI — NEW YORK

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UPLOADED
WITH/TEXT
WITH/OUTTEXT
BY
DATE 7-2-98

b6
b7C

AO93
(Rev.8/82)

SEARCH WARRANT ON WRITTEN AFFIDAVIT

COPY

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA v.	DOCKET NO. MAGISTRATE'S CASE NO. 98 1573M
THE PREMISES KNOWN AS:	TO: ANY SPECIAL AGENT OF THE FEDERAL BUREAU OF INVESTIGATION (FBI) OR ANY OTHER AUTHORIZED OFFICER

b6
b7C

Affidavit(s) having been made before me by the below-named affiant that he/she has reason to believe that on the premises known as SEE ATTACHMENT A

in the Central District of California

there is now being concealed certain property, namely: SEE ATTACHMENT B

and as I am satisfied that there is probable cause to believe that the property so described is being concealed on the person or premises above-described and the grounds for application for issuance of the search warrant exist as stated in the supporting affidavit(s).

YOU ARE HEREBY COMMANDED to search on or before ten (10) days (not to exceed 10 days) the person or place named above for the property specified, serving this warrant and making the search in the daytime--6:00 A.M. to 10:00 P.M. and if the property be found there to seize it, leaving a copy of this warrant and receipt for the property taken, and prepare a written inventory of the property seized and promptly return this warrant to the duty U.S. Magistrate Judge as required by law.

NAME OF AFFIANT	SIGNATURE U.S. MAGISTRATE JUDGE	DATE/TIME ISSUED
	RALPH ZAREFSKY	2:40 pm June 24, 1998

b6
b7C

*If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure Rule 41(c), show reasonable cause therefor.

**United States Judge or Judge of a State Court of Record.

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/17/98

[redacted] U.S. POSTAL INSPECTOR, 200 East Civic Centre Drive, 2nd Floor, Santa Anna, CA 92701 telephone number [redacted] was interviewed telephonically. After being advised of the identity of the interviewing agent and the nature of the interview, she provided the following information:

An updated P.O. Box application showed that [redacted]

b6
b7C

Express Mail package # EG315773469US was picked up by [redacted] on 06/09/98 at 10:12 a.m.

b3
b6
b7C
b7E

[redacted] 302

Investigation on 06/15/98 at New York, NY (tel[redacted]

File # [redacted] Date dictated 06/17/98

by SA [redacted]

JUN 2 2 1998

FBI — NEW YORK

[redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UPLOADED
WITH
VIA
BY [redacted] b6 b7C
DATE 11-2-98

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/15/1998

To: New York **Attn:** A/ASAC [redacted]
FMU - NYO

b3
b6
b7C
b7E

From: New York
Squad C37
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: Masters Of Downloading
Computer Crime - Intrusion

Synopsis: Request approval to pay for rental car expenses to be incurred by SA [redacted] during travel in Los Angeles, CA.

b6
b7C

Details: SA [redacted] was approved for travel to the Los Angeles division for the purposes of obtaining and executing a search warrant of premises occuppied by two subjects who are members of the Masters of Downloading, a computer hacker group. The group is believed to have obtained unauthorized access of US military computers and downloading sensitive information therefrom.

In order to conduct the necessary travel involved, including surveillance of location to be searched, travel to US Attorney's offices, FBI office, and other relevant location, it is necessary that SA [redacted] have ready access to a vehicle. FBI LA does not have a spare vehicle for this purpose. It is therefore requested that SA [redacted] receive approval to rent a car during captioned travel.

♦♦

[redacted]

SEARCHED [redacted] INDEXED
SERIALIZED [redacted] FILED [redacted]

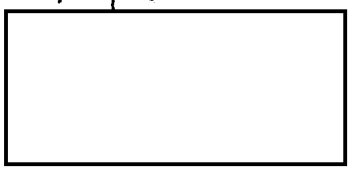
JUL 20 1998

[redacted]

b3
b6
b7C
b7E

UPLOADED
WITH ATTACHMENT
WITHOUT ATTACHMENT
BY [redacted]
DATE 7-21-98

FYI -



b6
b7C

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 07/24/1998

To: New York **Attn:** C-37
SA [redacted]

b3
b6
b7C
b7E

From: Los Angeles
WCC-3
Contact: SA [redacted] 310-996-3962

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted]

Title: [redacted] et al.;
DEFENSE INFORMATION SYSTEMS AGENCY
(DISA) - VICTIM;
CITA;
OO:NY

[redacted]

b3
b6
b7C
b7E

Synopsis: Lead covered in Los Angeles. Federal search warrant returned to magistrate as requested.

Reference: [redacted]

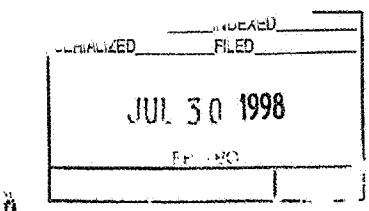
Administrative: Numerous telcals between SAs [redacted] and [redacted]

Attachment: Photocopy of the Return page of the Federal search warrant showing details of the return.

Details: On 07/06/1998 SA [redacted] returned the Federal search warrant and property receipts relating to the 06/26/1998 search of [redacted] to a Federal Magistrate in the Central District of California as requested in referenced serial. Lead covered.

SEARCHED [redacted]

♦♦



b6
b7C

RETURN

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH
June 24, 1998	June 26 1998 Approx 7:30 am	

INVENTORY MADE IN THE PRESENCE OF

INVENTORY OF PROPERTY TAKEN PURSUANT TO THE WARRANT

See attached (FD-597) Receipts for Property Seized. Eight pages FD-597 attached describing contents of seven (7) boxes which contain items seized and two (2) mini tower computers which were also seized from

b6
b7C

CERTIFICATION

I swear that this inventory [redacted] perty taken by me on the warrant.

b6
b7C

FBI

Subscribed, sworn to, and returned before me this date.

Roger Gregoire 7/6/98

U.S. JUDGE OR MAGISTRATE DATE

United States District Court

EASTERN DISTRICT OF NEW YORK

TO: [redacted]

SUBPOENA TO TESTIFY BEFORE GRAND JURY

SUBPOENA FOR: [redacted]

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

PLACE	ROOM	
United States District Court Eastern District of New York 225 Cadman Plaza East Brooklyn, New York 11201	478	b3 b6 b7C
	DATE AND TIME [redacted]	

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):*

[redacted]

☐ *Please see additional information on reverse*

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer acting on behalf of the court.

CLERK	DATE
Robert C. Heinemann	June 12, 1998
(BY) DEPUTY CLERK	

This subpoena is issued upon application of the United States of America	NAME, ADDRESS AND PHONE NUMBER OF ASSISTANT U.S. ATTORNEY
	[redacted] AUSA 147 Pierrepont Street Brooklyn, New York 11201 [redacted]

b6 b7C

*If not applicable, enter "none."

To be used in lieu of AO110

FORM OBD-027 JAN. 85

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/01/98

[redacted] was interviewed in the presence of his [redacted] at their residence. Also present during part of the interview was Special Agent [redacted] of the FEDERAL BUREAU OF INVESTIGATION (FBI), Los Angeles office. After being advised of the identity of the interviewing agents and the nature of the interview, he provided the following information: b6 b7C

[redacted] ran away from home in December 1997. [redacted] met [redacted] while he was a runaway and returned home with [redacted] in May 1998. [redacted] was allowed to stay at the residence. [redacted] and [redacted] worked at a telemarketing firm. b6 b7C

[redacted] admitted to being [redacted] and a member of the MASTERS OF DOWNLOADING (MOD). [redacted] admitted that he and [redacted] interviewed on the CBS EVENING NEWS that aired on May 20 & 26, 1998. b6 b7C

[redacted] advised that other [redacted] and others that he could not remember. [redacted] advised that he needed to look at his computer in order to recall more details. [redacted] was solely responsible for the web page hacking done by [redacted] admitted to hacking and defacing the [redacted] and [redacted] admitted to hacking and defacing [redacted] under the group name [redacted] hacked [redacted] with hackers known as [redacted] approximately 3 times and were from San Diego area. b6 b7C

[redacted] quit the [redacted] computer security team a few weeks ago. b3 b6 b7C b7E

A hacker known as [redacted] of MOD. Other members of MOD include members of [redacted] and [redacted]

Investigation on 06/26/98 at [redacted]

File # [redacted] Date dictated 07/01/98

by SA [redacted] DCIS SA [redacted] File: [redacted] 302

AUG 14 1998

FBI — NEW YORK

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UPLOADED
WITH/TEXT
WITH/OUT TEXT
BY
DATE 8-28-18
b6
b7C

known as [redacted] gives [redacted] new non-public hacking exploits. [redacted] often passes these exploits to other hacker he has working under him. [redacted] gave the statd exploit to [redacted] when it was not widely distributed. [redacted] b3 b6 b7C b7E

[redacted] believed that [redacted] is older than 18 years old. [redacted] has a static IP address and his [redacted] email account is [redacted] worked at computer networking company but was fired after he crashed the company network. [redacted] uses illegally obtained credit cards numbers (carding) to obtain Internet accounts and computer equipment. [redacted]

[redacted] denied taking or possessing the DEFENSE EQUIPMENT MANAGER (DEM) software. [redacted] knew that the DEM software was taken from an NT server. b6 b7C

[redacted] met someone named [redacted] who was associated with organized crime and was pirating CDS. [redacted] believed that [redacted] because of his IP address. [redacted] wanted to buy the DEM software. [redacted] told [redacted] that he could get the DEM software and to send him some money. [redacted] told [redacted] to send the money to [redacted] didn't think that [redacted] would send the money. [redacted] told [redacted] that he had an associate that wanted the DEM software that lived in the United States. [redacted] believed the associate lived in Brooklyn, New York or Boston. [redacted] received [redacted] money orders from [redacted] and a note with a pager number to call. [redacted] thought the DEM software was publicly available and planned to download the DEM from an anonymous FTP site. [redacted] was unable to get the DEM software. [redacted] lost the pager number and did not talk to the [redacted] told [redacted] that he could not get the DEM software. [redacted] believes that [redacted] is still expecting the software. [redacted] downloaded US Army documents from a public FTP site. [redacted] planned to send the documents to [redacted] so he could buy some time to get the DEM software. [redacted] did not send the US Army documents to [redacted] avoided the Undernet so that b6 b7C

he would not have to talk to [redacted]

In December 1997 [redacted] was contacted by a MICROSOFT administrator. [redacted] was asked to scan all of MICROSOFT's servers (*.microsoft.com) and identify weaknesses. [redacted] was not paid for the scanning. [redacted] was contacted by the system administrator at a nuclear lab and asked to scan the server for weaknesses. b6 b7C

[redacted] had one FTP site that he used at skynet.com. [redacted] had two shell accounts that he used. One shell was on a lonestar.net server and the other shell was located on a Japanese server which he could not recall.

[redacted] advised that he had hacking exploits on his computer. CORESCAN was a Windows 95/NT scanner that [redacted] was developing. [redacted] described CORESCAN as being faster than another scanner he developed called ORGE. [redacted] was developing another Windows 95/NT IP scanner called STATION1 or 0. It gave the user the ability to scan a host and identify a number of known exploits. [redacted] advised that he developed the SITESCAN2 scanner. b6 b7C

AFFIDAVIT FOR SEARCH WARRANT

COPY

UNITED STATES DISTRICT COURT	CENTRAL DISTRICT OF CALIFORNIA
UNITED STATES OF AMERICA VS.	DOCKET NO. MAGISTRATE CASE NO. 98 1573M
	NAME AND ADDRESS OF JUDGE 1 OR U.S. MAGISTRATE JUDGE HON. RALPH ZAREFSKY United States Magistrate Judge Los Angeles, California

b6
b7C

The undersigned being duly sworn deposes and says: That there is reason to believe that

☐ on the person of ☒ on the premises known as	CENTRAL DISTRICT OF CALIFORNIA

SEE ATTACHMENT A

The following property (or person) is concealed:

SEE ATTACHMENT B

Affiant alleges the following grounds for search and seizure 2

Evidence of violations of Title 18, United States Code, Sections 1029 and 1030.

☒ See attached affidavit which is incorporated as part of this affidavit for search warrant

Affiant states the following facts establishing the foregoing grounds for issuance of a Search Warrant

(SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED AS PART OF THIS AFFIDAVIT FOR SEARCH WARRANT)

SIGNATURE OF AFFIANT	OFFICIAL TITLE, IF ANY
	SPECIAL AGENT - FBI

Sworn to before me, and subscribed in my presence:

DATE	JUDGE OR US MAGISTRATE JUDGE
June 24, 1998	RALPH ZAREFSKY

1 United States Judge or Judge of a State Court of Record

2 If a search is to be authorized "at any time in the day or night" pursuant to Federal Rules of Criminal Procedure 41(c), show reasonable cause therefor.

b3
b6
b7C
b7E

AFFIDAVIT

I, [redacted] being duly sworn, hereby depose and say as follows: b6 b7C

1. I am a Special Agent for the Federal Bureau of Investigation ("FBI") assigned to the New York Field Office. I have been employed by the FBI as a Special Agent for approximately 1 year and my current duties include the investigation of computer related crimes. I have worked on a number of computer hacking cases; have received training in the methods of operation of computer hackers; have debriefed computer hackers relating to their hacking activities; have spoken with law enforcement officers with substantial experience in computer hacking cases regarding the methods of operation of computer hackers; and have received training, and have substantial personal experience, in the structure and operation of the Internet. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), as a Special Agent of the FBI.

2. The facts set forth below are based upon my own personal observations, information from confidential informants, reports made to me made by other law enforcement officers, and records I have obtained. I have not included in this affidavit all of the information I have uncovered relating to either the subjects of this investigation, their illegal activities, or the SUBJECT PREMISES. Rather, I have set forth in this affidavit only such facts as I have deemed necessary to establish probable cause to search the SUBJECT PREMISES.

3. Since April 1998, I have been participating in an investigation of [redacted] and [redacted] As set forth below [redacted] and [redacted] are computer "hackers." That is, using their computers, they gain unauthorized access to the computers of other persons and entities, often stealing data and programs from those computers. Both are members of a hacking organization called the "Masters of Downloading," or "MOD." My investigation has revealed that MOD hacked a Department of Defense ("DOD") computer (or "server") and stole certain non-classified DOD software, and that [redacted] claims to have possession of this software or to have access to this software. My investigation has further revealed that [redacted] have engaged in unauthorized intrusions into other computer systems.

b6
b7C

4. I make this affidavit in support of a warrant to search THE PREMISES KNOWN AND DESCRIBED AS [redacted] (including an attached garage) (hereafter referred to as the "SUBJECT PREMISES"). Based upon the facts set forth herein, there is probable cause to believe that evidence of violations of Title 18 U.S.C. §§ 1029 and 1030 and/or fruits or contraband of violations of these sections will be found at the SUBJECT PREMISES. In addition, I seek permission pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure to seize computer equipment and computer peripherals that constitute property used to commit a criminal offense.

b6
b7C

A. THE THEFT OF THE DEM SOFTWARE

5. AntiOnline is an Internet web site devoted to computer security issues, and it often contains stories regarding the illegal "hacking" of computers. Beginning on approximately April 21, 1998, AntiOnline posted a series of stories regarding an international group of hackers named the "Masters of Downloading," whose acronym was "MOD." The story was reportedly based on interviews with members of MOD, some of which were reportedly transcribed and posted. The MOD speakers were only identified as "MOD" and "MOD-2" in the interviews. During April and May 1998, I visited the AntiOnline web site and read the articles and interviews pertaining to the MOD intrusions. According to the interviews, the MOD speakers admitted to having "br[oken] into" a Department of Defense "server" belonging to the Defense Information System Agency ("DISA") in the fall of 1997. A "server" is a computer. DISA administers the military's telephone and computer communications systems.

6. In the articles, the MOD members claimed that they stole a software package from DISA called "DEM," which is an acronym for the Defense Information Systems Network Equipment Manager software. "DEM" software is non-public software that is installed on a very limited number of password-protected DISA computers, and is used in managing the DISA network of computers and telephones.

7. In the interviews, the MOD members claimed to have stolen from DISA computers "reports, logs of people using the

machines . . . reports on the status of routers and equipment . . . [and] network topologies for systems in the Pacific and Hawaii." They claimed to have gained "full root access to systems in [the United Systems], Hungary, Greece, Thailand, Japan, and China, around 350 in total." "Root access" means that the computer user is granted the highest level of access to any and all systems contained on a computer. Among other things, a user with "root access" has the ability to create accounts, change accounts and/or review any information stored on the computer.

8. As part of the stories, AntiOnline posted screen captures (that is, excerpts, as they appear on a computer screen) from the stolen DEM software that MOD had provided to AntiOnline. Brian Dumphy, a DISA official working at the DISA Global Operations Security Center, reviewed the screen captures and confirmed that they were accurate excerpts of the DEM software. In addition, [redacted] told me that DISA had recorded an unauthorized intrusion into a computer system that MOD claimed to have "hacked" around the same time that the MOD members claimed to have stolen the DEM software. According to [redacted] and [redacted] a civilian computer technician employed by DISA, the screen shots and the entire DEM software could not have been accessed by unauthorized personnel without the password protection being defeated in an illegal manner.

b6
b7C

9. In the AntiOnline interviews, the MOD members stated that they intended to "release" or "sell" the information they had

obtained from hacking military sites, and stated that "international terrorist groups would be interested in the data we could gain access to," and that "governments would buy it for intelligence purposes."

10. In the interviews, the MOD members also claimed to have obtained "classified information and access to networks" in the course of their hacking activities. The MOD speakers admitted to having "non-public local and remote exploits," a phrase generally used to refer to hacking "tools" or programs. They stated that they had "scanned" many systems throughout the world to obtain information regarding network weaknesses that would be useful in future hacking endeavors. The MOD speakers stated that they would "continue to infiltrate high-level U.S. governmental and military servers," and that they were involved in ongoing hacking activities involving the military computers of other countries. The MOD speakers believed that the stolen DEM software would enable them to remotely "take down," meaning disable, the "entire DISA network."

11. The MOD members also claimed to have stolen other "piece[s] of American military software" and "security programs from NASA . . . used for intrusion detection." The MOD speakers claimed to have "around 400 systems fully backdoored worldwide." A "backdoor" refers to a computer program installed by a hacker on a computer that allows the hacker to access the computer at a later time without having to defeat any existing or new computer security measures installed on the computer.

B. [redacted] CBS EVENING NEWS INTERVIEW

12. On May 20 and May 26, 1998, CBS Evening News telecast a two-part interview of two individuals who admitted they were part of MOD. I watched the CBS interview and reviewed a videotape copy of the interview. One individual identified himself only by the name [redacted] and the other individual identified himself only by the name [redacted] As set forth below, [redacted] and [redacted] have admitted being the two individuals interviewed in this broadcast. b6 b7C

13. In the CBS interviews, [redacted] admitted to being members of MOD. [redacted] stated that they "sit at [their] computers and use [their] phone lines to get into systems." [redacted] stated that they "steal" information from military systems. [redacted] stated that he was able to "insert some type of a backdoor . . . Trojan horse" on other computers. A "Trojan Horse" is a programming term of art that refers to a "backdoor" program. b6 b7C

14. In the CBS interviews, there was an attempt to black out the faces of [redacted] but their silhouettes were visible. At times, during the CBS interviews, [redacted] profile and goatee are visible. In an article posted to CBS's web site, the CBS interviewer identified [redacted] as [redacted] I have checked DMV records and NCIC records and confirmed that [redacted] are [redacted] [redacted] date of birth is [redacted] date of birth is [redacted] b6 b7C

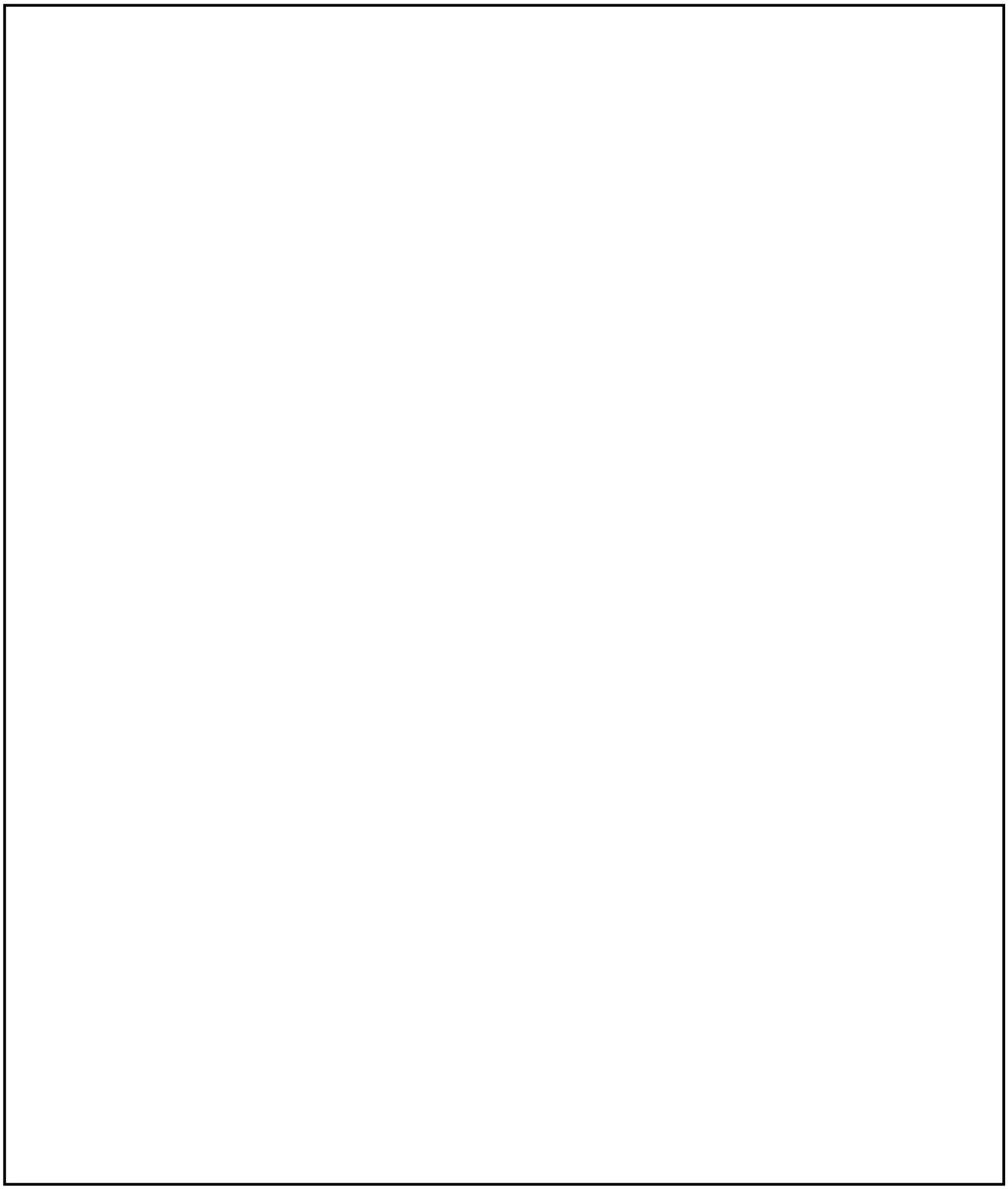
C. [redacted] NEGOTIATES TO SELL THE DEM SOFTWARE TO A CONFIDENTIAL SOURCE

15. Beginning in May 1998 and continuing to the present, I have been working with Special Agent [redacted] of the Defense Criminal Investigative Service ("DCIS"). SA [redacted] told me the following:

b6
b7C

[redacted]

b6
b7C
b7D
b7E



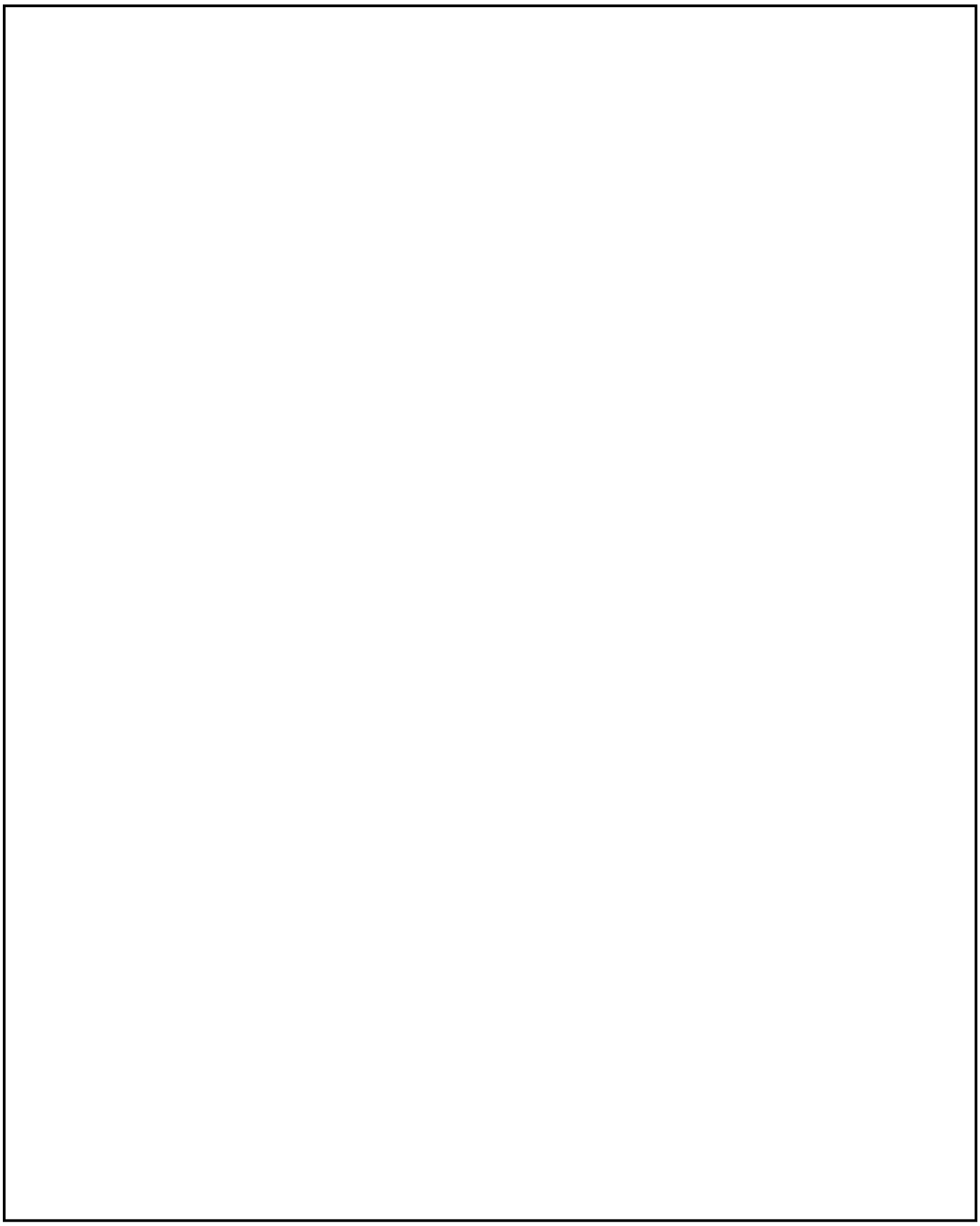
b6
b7C
b7D
b7E

D. TWO OTHER CONFIDENTIAL SOURCES OBSERVE COMPUTER HACKING TOOLS AND COMPUTERS USED FOR HACKING AT THE SUBJECT PREMISES

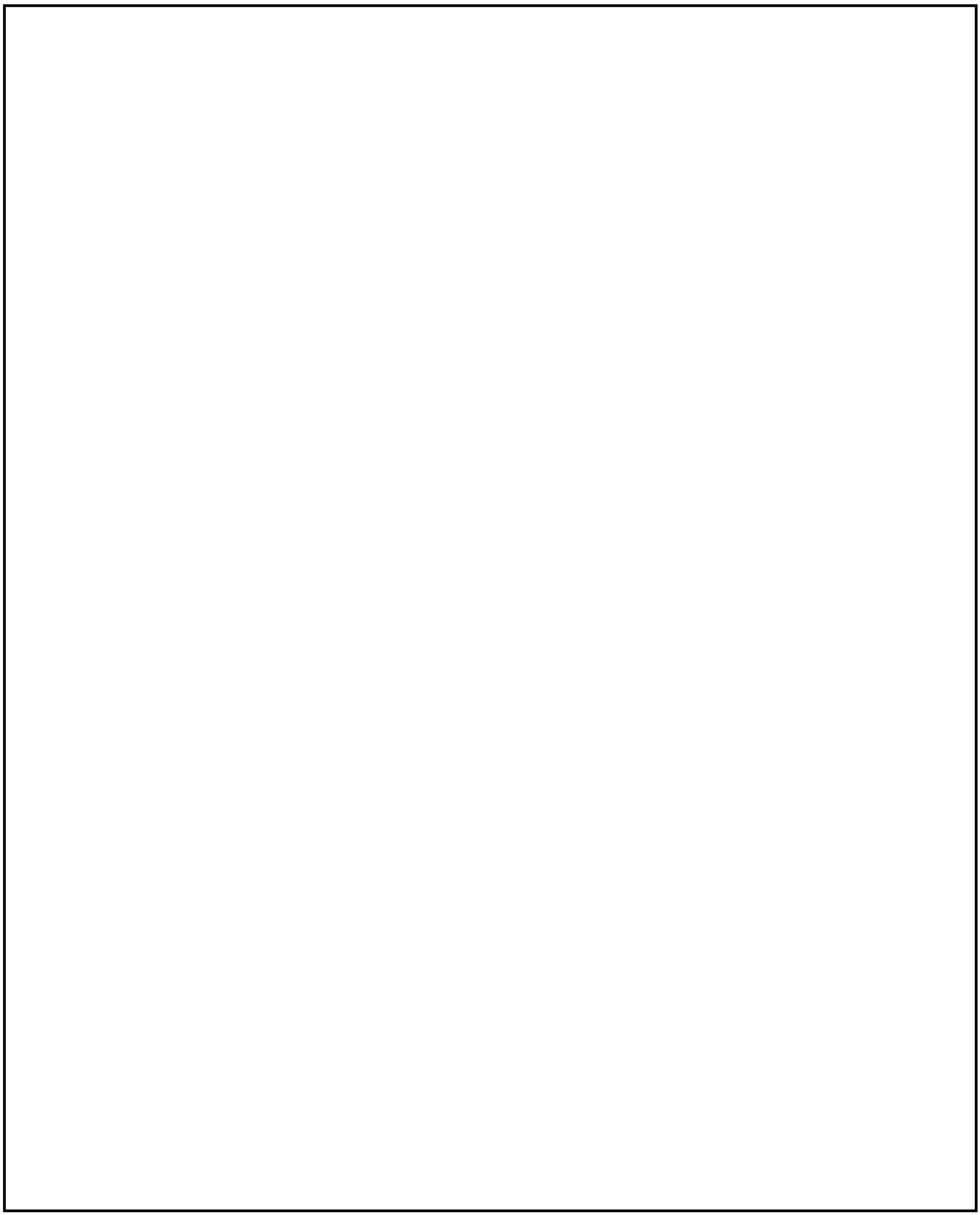
21. On or about June 21, 1998, I interviewed CS-2 and CS-3, who told me the following:

[redacted]

b6
b7C
b7D
b7E



b6
b7C
b7D
b7E



b6
b7C
b7D
b7E

[redacted]

b6
b7C
b7D
b7E

E. ITEMS TO BE SEIZED

25. Based on the foregoing, I respectively submit that there is probable cause to believe that concealed within the SUBJECT PREMISES are the following records, documents and materials:

a. Records, documents, programs, applications and materials which reflect hacking activities, including copies of stolen DEM software; copies of other stolen military, governmental, or commercial software, data, and information; "hacking" tools and programs; lists of usernames; passwords; credit card numbers; computerized logs; account names; personal telephone books; personal address books; exploits and other hacking programs; videotape of May 20, 1998 and May 26, 1998 C.B.S. Evening News interviews; and documents retrieved from the trash receptacles of computer companies;

b. Computing or data processing literature, including printed copy, instruction books, papers, or listed computer programs in whole or in part;

c. Computers; central processing units; external and internal drives; external and internal storage equipment or media; terminals or video display units; computer software; computerized data storage devices, including data stored on hard disks or floppy disks, computer printouts, and computer programs; computer or data processing software or data including: hard disks, floppy disks, cassette tapes, video cassette tapes and magnetic tapes, together with peripheral equipment such as keyboards, printers, modems or acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, telephone blue boxes, and magnetic tapes which could contain or be used to transmit or store any of the foregoing records, documents and materials;

d. Indicia of occupancy, including: bills, letters, invoices, personal effects, and rental agreements tending to show ownership, occupancy, or control of the premises or the above-described items; and

e. Records, documents and materials which refer, relate to, or are for use in, computer hacking. As used herein, the terms records, documents and materials includes records and documents created, modified or stored in electronic or magnetic form and any data, image, or information that is capable of being read or interpreted by a computer.

26. In order to search for any items to be seized that were prepared, modified, or stored in electronic or magnetic form, searching agents may seize and search the following:

a. Any computer hardware or computer-related equipment capable of creating or storing information in electronic or magnetic form;

b. Any computer peripheral used to facilitate the transmission, creation, display, encoding or storage of information, images and data including word processing equipment, modems, monitors, printers, plotters, encryption circuit boards, optical scanners;

c. Any magnetic or electronic storage device such as floppy diskettes, hard disks, backup tapes, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks;

d. Computer software, documentation, operating logs and instruction manuals relating to the operation of the computer hardware and software to be searched;

e. Application software, utility programs, compilers, interpreters, and other programs or software used to facilitate direct or indirect communication with the computer hardware and software to be searched;

f. Any physical keys, encryption devices and similar physical items that are necessary to gain access to the computers to be searched or are necessary to gain access to the programs, data, and information contained on the computer to be searched;

g. Any passwords, password files, test keys, encryption codes or other computer codes necessary to access the computers to be searched or to convert any data, file or

information on the computers into a readable form;

h. Electronically stored communications or messages, including any of the items to be seized that may be found in electronic mail ("e-mail").

F. REQUEST TO SEIZE COMPUTER EQUIPMENT AND COMPUTER PERIPHERALS PURSUANT TO RULE 41(b)

27. Based upon the facts set forth herein, there is probable cause to believe that the computer equipment and computer peripherals currently located at the SUBJECT PREMISES is property which "is or has been used as the means of committing a criminal offense," namely, violations of Title 18 U.S.C. §§ 1029 and 1030.

28. Accordingly, pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure, searching agents respectfully request permission to seize any computers or computer peripherals, including computer hardware or computer-related equipment capable of creating or storing information in electronic or magnetic form. Such computer equipment shall include central processing units; external and internal drives; external and internal storage equipment or media; terminals or video display units. Such computer peripherals shall include keyboards, printers, modems or acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and telephone blue boxes.

29. In addition, there is probable cause to believe that certain items located at the SUBJECT PREMISES constitute

"property that constitutes evidence of the commission of a criminal offense" or "contraband, the faits of crime, or things otherwise criminally possessed" within the meaning of Fed. R. Crim. P. 41(b)(1) and (2). Accordingly, searching agents request permission to seize any contraband, property or fruits of crime, including electronic files, obtained in violation of 18 U.S.C. §§ 1029 and 1030.

G. METHODS TO BE USED TO SEARCH COMPUTERS

30. Based upon my training and experience, I know that searching computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored. It would be

impractical to attempt this kind of data search on site.

b. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code embedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

31. If, after inspecting the input/output devices, software, documentation, and data security devices, the analyst determines that these items are no longer necessary to retrieve and preserve the data evidence, and that any such item is not otherwise subject to seizure pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure, the government will return these items within a reasonable period of time not to exceed 60 days.

32. It may be necessary for programmers and other outside experts to assist the FBI during the examination of the computer

evidence in order to help identify ownership and trace the programs, other property, or codes stolen from the victim computer system and to determine the full extent and nature of the unauthorized intrusions into the victim computer system.

I declare under penalty of perjury that the foregoing is true and correct.

[redacted]

b6
b7C

Special Agent
Federal Bureau of
Investigation

Sworn to before me this
24th day of June 1998

RALPH ZAREFSKY
UNITED STATES MAGISTRATE-JUDGE

RETURN

DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH

INVENTORY MADE IN THE PRESENCE OF

INVENTORY OF PROPERTY TAKEN PURSUANT TO THE WARRANT

CERTIFICATION

I swear that this inventory is a true and detailed account of all the property taken by me on the warrant.

_____

Subscribed, sworn to, and returned before me this date.

_____

U.S. JUDGE OR MAGISTRATE **DATE**

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 7/28/98

On July 23, 1998, at Northridge, California, an Abacus laptop computer, serial# TN83003647, with a PC modem card, serial# 28J30693T was received as evidence from Group Manager [redacted] Defense Criminal Investigative Service.

Special Agent [redacted] related that [redacted] had voluntarily surrendered the above described laptop belonging to [redacted] to the Defense Criminal Investigative Service, on June 29, 1998.

b6
b7C

Investigation on 7/23/98 at Northridge, CA [redacted]

b3
b6
b7C
b7E

File # [redacted] Date dictated

by SA [redacted]

SEP 2 6 1998

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 7/24/98

Examined on this date were the following:

LA-3:
Abacus laptop computer, serial# TN83003647 with a 2.1 GB Toshiba model MK2104MAV hard drive, serial# 28J30693T; PC modem card, serial# 752C79501502, and a 3½ inch floppy drive.

LA-4:
125 MB Seagate model ST3144A hard drive, serial# 911006-005.

LA-5:
125 MB Seagate model ST1144A hard drive, serial# 00K0S529472.

LA-6:
341 MB Western Digital Caviar model 2340 hard drive.

LA-7:
540 MB Maxtor model MXT-540A hard drive, serial# 752039005M.

LA-8:
203 MB Maxtor model 7213AT hard drive, serial# B10350AS.

LA-9:
1.6 GB Western Digital Caviar model 21600, serial# WM3364344424.

LA-10:
CD-ROM entitled, "Slackware 3.4".

LA-11:
85 MB Conner model CP30084E hard drive, serial# ALB4BkB.

LA-12 through LA-46:
3½ inch floppy disks

b6
b7C

b3
b6
b7C
b7E

Investigation on 7/23/98 at Northridge, CA

File # [redacted]

by SA [redacted] SA [redacted] SA [redacted] SA [redacted] (DCIS), SA [redacted] (DCIS)

7/24/98 Swanson

SEP 2 0 1998

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

LA-47:
CD-ROM

LA-48 through LA-108:
3½ inch floppy disks

LA-109 through LA-125:
5¼ inch floppy disks

LA-126 and LA-127:
3½ inch floppy disks

Results of Examination:

Items LA-3 through LA-127 were accessed using the computer resources currently available to the Federal Bureau of Investigation, Los Angeles Field Office and the Los Angeles office of the Defense Criminal Investigative Service.

LA-3 utilized a BIOS password. The hard drive was removed and imaged.

LA-4, LA-5, LA-8, LA-9, and LA-11 were each imaged.

LA-6 and LA-7 were not readable.

CD-ROMs LA-10 and LA-47 were copied.

Floppy disks LA-12 through LA-16, LA-18 through LA-46, LA-48 through LA-111, LA-113 through LA-117, LA-119 through LA-122, and LA-125 through LA-127 were copied.

Floppy disks LA-46, and LA-48 through LA-54 were formatted for Linux.

Floppy disks LA-17, LA-112, LA-118, LA-123 and LA-124 were unreadable.

REMARKS

The images of LA-3 through LA-5, LA-8, LA-9, and LA-11 were copied. The original images were provided to Defense

[redacted]

b3
b6
b7C
b7E

Criminal Investigative Service. The copies were submitted as evidence.

The copies of the CD-ROMs and floppy diskettes were given to Defense Criminal Investigative Service.

Notes of the examination were submitted as evidence.